

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2002 年 3 月 21 日 (21.03.2002)

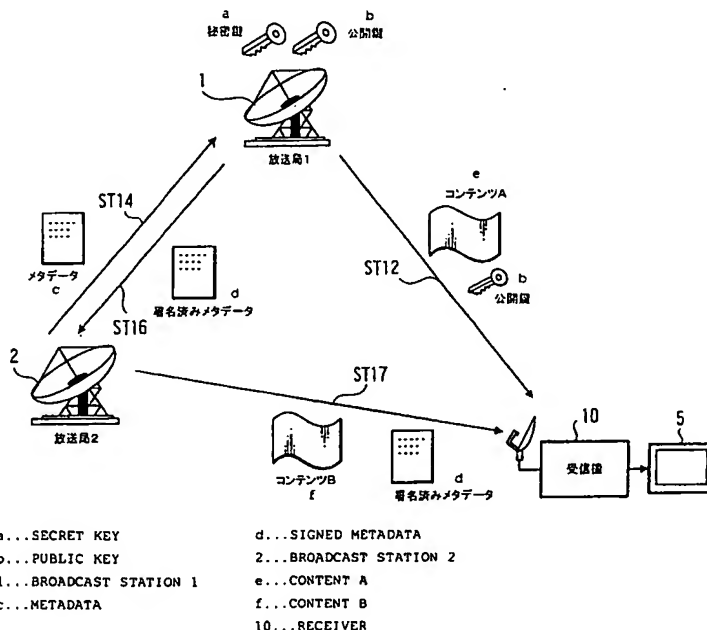
PCT

(10) 国際公開番号
WO 02/23903 A1

- (51) 国際特許分類⁷: H04N 7/16 (ASADU, Hideki) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP01/07924
- (22) 国際出願日: 2001 年 9 月 12 日 (12.09.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願2000-277177 2000 年 9 月 12 日 (12.09.2000) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 浅津英樹
- (74) 代理人: 弁理士 松隈秀盛 (MATSUKUMA, Hide-mori); 〒160-0023 東京都新宿区西新宿1丁目8番1号 新宿ビル Tokyo (JP).
- (81) 指定国 (国内): CN, JP, KR, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- 添付公開書類:
— 国際調査報告書
- 2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: INFORMATION PROCESSING DEVICE, ELECTRONIC DEVICE, INFORMATION PROCESSING METHOD, AND MEDIUM

(54) 発明の名称: 情報処理装置、電子機器、情報処理方法及び媒体



(57) Abstract: When a first content previously distributed is referred to in relation to a second content, the limit on the use of the first content effectively functions. A secret key and a public key are generated for the first content, and the first content to which the public

[続葉有]



key is added is transmitted. When a second content for which the user wants to refer to the second content is generated, the manager managing the first content is requested to sign predetermined data added to the second content by means of the secret key generated when the first content is broadcast. After the signature, the second content to which the signed predetermined data is added is transmitted. On the receiving side, collation of the signature on the predetermined data is performed by means of the public key added to the first content. If the collation succeeds, the stored first content is subjected to a predetermined processing according to the instruction of the second content and outputted.

(57) 要約:

過去に配信された第 1 のコンテンツを、第 2 のコンテンツが参照する処理を行う際に、その第 1 のコンテンツの利用制限が有効に機能にするようにする。このために、第 1 のコンテンツに対して、秘密鍵と公開鍵を生成させ、その公開鍵を付加して、第 1 のコンテンツを送信し、その後、第 1 のコンテンツを参照したい第 2 のコンテンツが発生したとき、第 2 のコンテンツに付加される所定データに対して、第 1 のコンテンツ放送時に生成させた秘密鍵での署名を、第 1 のコンテンツの管理者に要求し、その署名が行われたとき、その署名された所定データが付加された第 2 のコンテンツを送信する。受信側では、第 1 のコンテンツに付加された公開鍵を使用して、第 2 のコンテンツに付加された所定データの署名を照合する処理を行い、照合に成功したとき、第 2 のコンテンツの指示に基づいて、蓄積された第 1 のコンテンツに所定の加工を施して出力する。

明 細 書

情報処理装置、電子機器、情報処理方法及び媒体

技術分野

- 5 本発明は、例えばテレビジョン放送の番組などのコンテンツを送信して受信する情報処理方法と、その情報処理方法を適用した情報処理装置及び電子機器、並びに情報処理方法が実行されるプログラムが格納又は伝送される媒体に関する。

10 背景技術

- 従来、テレビジョン放送は、その放送を受信したときに、その放送を受信した受信機に接続（又は一体化）された受像機で、リアルタイムにその放送番組を視聴するか、或いはビデオテープレコーダなどの記録再生装置で、その番組を一旦記録し、その記録
15 されたテープなどを任意の時間に再生させて視聴することが行われていた。

- いずれの場合でも、従来は基本的には受信した番組をそのまま視聴するだけであり、例えばビデオテープに記録させて再生する際に、早送りなどを送って一部を飛ばすことができる程度であった。
20

- これに対して、近年、ディスク（ハードディスク、光ディスク、光磁気ディスクなど）を媒体とした記録再生装置の性能の向上やコストの低下に伴って、放送信号の受信機に、ディスク記録再生装置を内蔵させて、受信した放送番組のデータを内蔵されたディスク記録再生装置に記録させておき、その記録された番組データをユーザが任意の時間に再生させることが可能になりつつある。
25

この場合、ディスク記録再生装置の場合には、記録された任意

のデータへのアクセスが容易であるため、ユーザの操作に基づいて、任意の形態で再生させるようにすることも可能である。

5 一方、放送局からデジタルデータで番組データが伝送されるいわゆるデジタル放送の場合には、番組内容そのもののデータであるコンテンツデータの他に、各種データを付加して伝送することが可能であり、その付加データを使用して、デジタル記録再生装置に記録されたコンテンツデータの再生形態を指示するようなことも考えられている。

10 例えば、ある特定の番組（コンテンツ A とする）が放送されたとき、そのコンテンツ A をあるユーザの受信機に内蔵された記録装置で記録させたとする。その後、別の番組（コンテンツ B とする）が放送されたときに、コンテンツ A が受信機内に蓄積されたユーザに対しては、コンテンツ A の一部の画像などを、コンテンツ B の視聴時に参照させることを指示するデータを放送局側から
15 送り、そのデータに基づいて、各ユーザの受像機では、例えばコンテンツ A の画像とコンテンツ B の画像とを合成して表示させることを実現させることが提案されている。このような放送局側から送られるデータに基づいた指示で、表示形態などが設定される場合には、基本的にはユーザは特別な操作を必要としない。

20 このようにすることで、過去に放送したコンテンツを有効活用した新たなコンテンツを生成させることが可能になり、テレビジョン放送などの新たな利用形態を作り上げることができる。

しかしながら、過去に放送されたコンテンツ A を、別のコンテンツ B の視聴時に加工利用するようにすること、コンテンツ A の
25 製作者や放送業者の権利を侵害するおそれがある。このため、このような過去の蓄積されたコンテンツを利用する場合には、何らかの制限を設けて、コンテンツ A の著作権者などを侵害しないような処理が必要である。

既に提案されている過去のコンテンツの利用制限処理としては、例えば、コンテンツ A を放送する際に、そのコンテンツ A を参照することを許可したコンテンツのリスト（アクセスコントロールリスト）のデータを配信することが考えられている。ところが、
5 コンテンツ A を放送した時点で、将来そのコンテンツ A が他のコンテンツでどのように利用されるのかを予測するのは困難であり、コンテンツ A を配信する際に、参照可能なコンテンツの完全なリストのデータを作成するのは困難である問題がある。

このためには、コンテンツ A のアクセスコントロールリストを将来に渡って更新させることも考えられるが、過去に配信された個々のコンテンツのアクセスコントロールリストを個別に管理させて更新させることは、管理コストなどを考えると現実的ではない。
10

15 発明の開示

本発明は、過去に配信されたコンテンツを、別のコンテンツが参照する処理を行う際に、その過去のコンテンツの利用制限が有効に機能にできるようにすることを目的とする。

第 1 の発明は、ネットワークを介して情報の授受を行う情報処理装置において、
20

上記第 1 のコンテンツに対して、秘密鍵と公開鍵を生成させて管理する鍵管理手段と、

上記鍵管理手段で管理する公開鍵を付加して、上記第 1 のコンテンツを送信する第 1 の送信手段と、

25 上記第 2 のコンテンツに付加される所定データに対して、上記鍵管理手段が管理する秘密鍵での電子署名を要求し、その電子署名された所定データが付加された上記第 2 のコンテンツを送信する第 2 の送信手段とを備えたものである。

このようにしたことによって、第 1 のコンテンツの管理者に参照することが許可された場合にだけ、正しい署名が行われた所定データが第 2 のコンテンツに付加されるので、第 1 のコンテンツを蓄積した各受信者側の設備では、第 1 のコンテンツを参照して
5 も良いと許可されたコンテンツを受信したときだけ、自動的に別のコンテンツが第 1 のコンテンツを参照するようになる。従って、過去のコンテンツの製作者や放送業者の権利を守った上で、随時その過去のコンテンツを参照した新たなコンテンツを制作して配信できるようになる。

10 第 2 の発明は、第 1 の発明の情報処理装置において、

上記鍵管理手段は、上記第 2 の送信手段からの電子署名要求時に、上記第 2 のコンテンツによる第 1 のコンテンツの参照が、第 1 のコンテンツの所定の権利を侵害しないと判断したときだけ、上記所定データへの電子署名を実行するようにしたものである。

15 このようにしたことによって、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツの一部を利用した別のコンテンツを作成して視聴させることができるようになる。

20 第 3 の発明は、ネットワークを介して情報の授受を行う情報処理装置において、

第 1 のコンテンツと、第 1 のコンテンツに関連する所定データとを、第 2 のコンテンツに適用される秘密鍵を用いて上記所定データに電子署名を行った電子署名データに組み合わせて送信する第 1 の送信手段を備えたものである。このようにしたことによって、例えば第 1 のコンテンツを送信する場合に、既に放送などが
25 行われた第 2 のコンテンツを利用を許可するデータを良好に送信できるようになる。

第 4 の発明は、第 3 の発明の情報処理装置において、

上記電子署名データを取得する電子署名データ取得手段を有するものである。このようにしたことによって、例えば、離れた場所で電子署名された電子署名データを取得できるようになる。

第5の発明は、第3の発明の情報処理装置において、

5 上記秘密鍵を使用して電子署名が行われる上記所定データは、
上記第2のコンテンツの参照命令を含むようにしたものである。
このようにしたことによって、例えば、第1のコンテンツを出力
させる際に、必ず第2のコンテンツを参照するようになり、第1
のコンテンツだけが出力されるようなことを防止できる。

10 第6の発明は、第5の発明の情報処理装置において、

 上記所定データは、第1のコンテンツに対する挿入開始位置情
報、挿入終了位置情報及び対応する第2のコンテンツの参照開始
位置情報、参照終了位置情報を有するものである。このようにし
たことによって、第1のコンテンツの第2のコンテンツへの挿入
15 が、決められた位置に行われるようになる。

 第7の発明は、

 コンテンツデータを受信する受信手段と、

 上記受信手段が受信したコンテンツを蓄積するコンテンツ蓄積
手段と、

20 上記コンテンツ蓄積手段に蓄積された第1のコンテンツに付加
された鍵データを使用して、上記受信手段が受信した第2のコン
テンツに付加された所定データの電子署名を照合する照合手段と

 、
 上記照合手段での照合が成功したとき、上記コンテンツ蓄積手
25 段に蓄積された第1のコンテンツを、上記第2のコンテンツでの
指示に基づいて加工するコンテンツ加工手段と、

 上記コンテンツ加工手段で加工されたコンテンツを出力するコ
ンテンツ出力手段とを備えた電子機器としたものである。このよ

うにしたことによって、第 1 のコンテンツを参照しても良いと許可されたコンテンツを受信したときだけ、自動的に別のコンテンツが第 1 のコンテンツを参照するようになる。従って、過去のコンテンツの製作者や放送業者の権利を守った上で、随時その過去のコンテンツを参照した新たなコンテンツを制作して配信できるようになる。

第 8 の発明は、第 7 の発明の電子機器において、

上記コンテンツ加工手段での加工は、上記第 1 のコンテンツによる画像又は音声と上記第 2 のコンテンツによる画像又は音声を合成する処理としたものである。このようにしたことによって、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツの画像又は音声と、後から送信されたコンテンツとの画像又は音声とを合成させて視聴又は聴取させることができるようになる。

第 9 の発明は、第 7 の発明の電子機器において、

上記コンテンツ加工手段での加工は、上記第 1 のコンテンツによる画像又は音声の一部を、上記第 2 のコンテンツによる画像又は音声に置き替える処理としたものである。このようにしたことによって、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツの一部の画像や音声などを最新のデータに置き替えて視聴させることができるようになる。

第 10 の発明は、第 7 の発明の電子機器において、

上記コンテンツ加工手段での加工は、上記第 1 のコンテンツによる画像又は音声を、第 2 のコンテンツによる指示で編集する処理としたものである。このようにしたことによって、過去のコンテンツの管理者に許可された場合にだけ、例えば、過去の特定のコンテンツのハイライトシーンだけを表示させるようなことが可能になる。

第 1 1 の発明は、ネットワークを介して情報の授受を行い、それら情報を記録及び／又は再生する電子機器において、

5 第 1 のコンテンツと、上記第 1 のコンテンツに関連する第 1 の所定データと、第 2 のコンテンツに適用される秘密鍵を上記第 1 の所定データに用い生成された電子署名データとの組み合わせデータを受信する第 1 の受信手段を有するものである。このようにしたことによって、例えば第 1 のコンテンツを受信した場合に、既に放送などが行われた第 2 のコンテンツを利用を許可するデータを良好に受信できるようになる。

10 第 1 2 の発明は、第 1 1 の発明の電子機器において、

上記秘密鍵を使用して電子署名が行われる上記第 1 の所定データは、第 2 のコンテンツの参照命令を含むものである。このようにしたことによって、第 1 のコンテンツを受信したとき、確実に第 2 のコンテンツを参照するようになる。

15 第 1 3 の発明は、第 1 2 の発明の電子機器において、

上記第 1 の所定データは、第 1 のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第 2 のコンテンツの参照開始位置情報、参照終了位置情報を有するものである。このようにしたことによって、第 1 のコンテンツの第 2 のコンテンツへの挿入が、決められた位置に行われるようになる。

20 第 1 4 の発明は、第 1 1 の発明の電子機器において、

第 2 のコンテンツと上記秘密鍵に対応する公開鍵とを受信する第 2 の受信手段と、

25 受信された上記第 2 のコンテンツと上記公開鍵を記憶する記憶手段とを有するものである。このようにしたことによって、記憶手段に記憶された第 2 のコンテンツと公開鍵とを利用して処理できるようになる。

第 1 5 の発明は、第 1 4 の発明の電子機器において、

上記電子署名データを上記公開鍵を用い復号化し、復号化データを生成する復号化手段と、

上記第 1 の所定データを所定のアルゴリズムに基づいて第 2 の所定データに変換するデータ変換手段と、

5 上記復号化手段により生成された上記復号化データと、上記データ変換手段により変換された上記第 2 の所定データとを照合する照合手段とを有するものである。このようにしたことによって、照合で一致した場合にだけ、記憶した第 2 のコンテンツを利用できるようになる。

10 第 1.6 の発明は、第 1.5 の発明の電子機器において、

 上記照合手段の照合結果が一致した場合、上記第 1 の所定データに基づき上記記憶手段に記憶された第 2 のコンテンツを所定のタイミングで参照する参照手段とを有するものである。このようにしたことによって、第 2 のコンテンツを参照することが、確実に
15 行えるようになる。

 第 1.7 の発明は、第 1 のコンテンツと、この第 1 のコンテンツを参照する第 2 のコンテンツを処理する情報処理方法において、

 上記第 1 のコンテンツに対して、秘密鍵と公開鍵を生成させ、
 上記生成された公開鍵を付加して、上記第 1 のコンテンツを送
20 信し、

 上記第 2 のコンテンツに付加される所定データに対して、上記秘密鍵での電子署名を要求し、

 上記電子署名された所定データが付加された上記第 2 のコンテンツを送信するものである。このようにしたことによって、第 1
25 のコンテンツの管理者に参照することが許可された場合にだけ、正しい署名が行われた所定データが第 2 のコンテンツに付加されるので、第 1 のコンテンツを蓄積した各受信者側の設備では、第 1 のコンテンツを参照しても良いと許可されたコンテンツを受信

したときだけ、自動的に別のコンテンツが第 1 のコンテンツを参照するようになる。従って、過去のコンテンツの製作者や放送業者の権利を守った上で、随時その過去のコンテンツを参照した新たなコンテンツを制作して配信できるようになる。

5 第 18 の発明は、第 17 の発明の情報処理方法において、
送信される上記第 1 のコンテンツを受信して蓄積した状態で、
送信される上記第 2 のコンテンツを受信した場合に、蓄積された
第 1 のコンテンツに付加された公開鍵を使用して、上記所定デー
タの電子署名を照合し、

10 その照合に成功したとき、受信した上記第 2 のコンテンツの指示に基づいて、上記蓄積された第 1 のコンテンツに所定の加工を施して出力するものである。このようにしたことによって、過去に受信した第 1 のコンテンツを利用して第 2 のコンテンツを出力させることが、良好に行える。

15 第 19 の発明は、ネットワークを介して情報の授受を行う情報処理方法において、

第 1 のコンテンツと、第 1 のコンテンツに関連する所定データとを送信する場合に、

20 上記第 1 のコンテンツとは別の第 2 のコンテンツに適用される秘密鍵を用いて、上記所定データに電子署名を行い、

その電子署名された電子署名データを上記所定データに組み合わせて送信するものである。このようにしたことによって、例えば第 1 のコンテンツを送信する場合に、既に放送などが行われた第 2 のコンテンツを利用を許可するデータを良好に送信できるようになる。

25 第 20 の発明は、第 19 の発明の情報処理方法において、

上記秘密鍵を用いた電子署名を、上記第 2 のコンテンツ又は上記秘密鍵を管理する側に依頼し、その依頼に基づいて得られた電

子署名データを、上記所定データに組み合わせるようにしたものである。このようにしたことによって、例えば、離れた場所で電子署名された電子署名データを取得できるようになる。

第 2 1 の発明は、第 1 9 の発明の情報処理方法において、

5 上記秘密鍵を使用して電子署名が行われる上記所定データは、
上記第 2 のコンテンツの参照命令を含むようにしたものである。
このようにしたことによって、例えば、第 1 のコンテンツを出力
させる際に、必ず第 2 のコンテンツを参照するようになり、第 1
のコンテンツだけを出力させるようなことを防止できる。

10 第 2 2 の発明は、第 2 1 の発明の情報処理方法において、

 上記所定データは、第 1 のコンテンツに対する挿入開始位置情
報、挿入終了位置情報及び対応する第 2 のコンテンツの参照開始
位置情報、参照終了位置情報を有するものである。このようにし
たことによって、第 1 のコンテンツの第 2 のコンテンツへの挿入
15 が、決められた位置に行われるようになる。

 第 2 3 の発明は、ネットワークを介して情報の授受を行い、そ
れら情報を記録及び／又は再生する情報処理方法において、

 第 1 のコンテンツを記録するとき、上記第 1 のコンテンツに関
連する第 1 の所定データと、既に記録された第 2 のコンテンツに
20 適用される秘密鍵を上記第 1 の所定データに用い生成された電子
署名データとを記録するものである。このようにしたことによっ
て、第 2 のコンテンツを参照することを指示するデータを良好に
記録できるようになる。

 第 2 4 の発明は、第 2 3 の発明の情報処理方法において、

25 上記秘密鍵を使用して電子署名が行われる上記第 1 の所定デ
ータは、第 2 のコンテンツの参照命令を含むようにしたものである
。このようにしたことによって、例えば、第 1 のコンテンツを出力
させる際に、必ず第 2 のコンテンツを参照するようになり、第

1 のコンテンツだけが出力されるようなことを防止できる。

第 2 5 の発明は、第 2 3 の発明の情報処理方法において、

5 上記第 1 の所定データは、第 1 のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第 2 のコンテンツの参照開始位置情報、参照終了位置情報を有するものである。このようにしたことによって、第 1 のコンテンツの第 2 のコンテンツへの挿入が、決められた位置に行われるようになる。

第 2 6 の発明は、第 2 3 の発明の情報処理方法において、

10 第 2 のコンテンツと上記秘密鍵に対応する公開鍵とを受信したとき、受信された上記第 2 のコンテンツと上記公開鍵を記録するようにしたものである。このようにしたことによって、その第 2 のコンテンツを利用する第 1 のコンテンツを受信したときに、記録された公開鍵と第 2 のコンテンツのデータを利用した処理が確実に実行できるようになる。

15 第 2 7 の発明は、第 2 6 の発明の情報処理方法において、

上記電子署名データを上記公開鍵を用い復号化し、復号化データを生成し、

上記第 1 の所定データを所定のアルゴリズムに基づいて第 2 の所定データに変換し、

20 上記復号化データと上記第 2 の所定データとを照合するようにしたものである。このようにしたことによって、照合で一致した場合にだけ、記憶した第 2 のコンテンツを利用できるようになる。

第 2 8 の発明は、第 2 7 の発明の情報処理方法において、

25 上記照合の結果が一致した場合、上記第 1 の所定データに基づき、既に記録された第 2 のコンテンツを所定のタイミングで参照するようにしたものである。このようにしたことによって、第 2 のコンテンツを参照することが、確実に行えるようになる。

図面の簡単な説明

図 1 は、本発明の一実施の形態による放送システムの全体構成の例を示す構成図である。

5 図 2 は、本発明の一実施の形態によるシステムに適用される放送局の構成例を示すブロック図である。

図 3 は、本発明の一実施の形態によるシステムに適用される受信機の構成例を示すブロック図である。

図 4 は、図 3 に示した受信機をデータ処理上から見た構成で示したブロック図である。

10 図 5 は、本発明の一実施の形態による放送動作と受信動作を時間の流れで示した図である。

図 6 は、図 5 に示した処理を、データの流れで示した説明図である。

15 図 7 は、秘密鍵と公開鍵を使用した処理例を示した説明図である。

図 8 は、本発明の一実施の形態により過去のコンテンツを利用する例（番組紹介を行う例）を示した説明図である。

図 9 は、図 8 の例による処理を示したフローチャートである。

20 図 10 は、本発明の一実施の形態により過去のコンテンツを利用する例（CMを差し替える例）を示した説明図である。

図 11 は、図 10 の例による処理を示したフローチャートである。

図 12 は、本発明の他の実施の形態による放送システムの全体構成の例を示す構成図である。

25 図 13 は、図 12 の例のシステムに適用される放送局の構成例を示すブロック図である。

図 14 は、図 12 の例のシステムに適用される鍵サーバの構成例を示すブロック図である。

図 1 5 は、本発明の他の実施の形態による放送動作と受信動作を時間の流れで示した図である。

図 1 6 は、図 1 2 に示した処理を、データの流れで示した説明図である。

5

発明を実施するための最良の形態

以下、本発明の一実施の形態を、図 1 ～図 1 1 を参照して説明する。

10 図 1 は本例の放送システムの全体構成例を示した図である。本例においては、衛星放送によるテレビジョン放送システムに適用した例としてあり、ここでは第 1 の放送局 1 と第 2 の放送局 2 とが用意されて、両放送局 1, 2 は何らかのネットワーク 3 で接続されている。このネットワーク 3 については、どのような通信手段であっても良く、電話回線、専用通信回線などが適用可能である。或いは、ネットワーク 3 として、インターネットや電子メールによるデータ伝送を利用しても良い。

15

20

25

第 1 の放送局 1 と第 2 の放送局 2 は、人工衛星 4 に対して所定のアップリンクで放送データが無線送信し、人工衛星 4 からのダウンリンクで各ユーザ側に設置された受信機 1 0 に対して放送データを無線送信し、放送局 1, 2 からの各種コンテンツ（番組）を、例えば各放送局毎に割当てられたチャンネルを使用して送信する。ここでは、受信機 1 0 に接続された受像機 5 で、受信した放送の視聴を行う構成としてある。本例の受信機 1 0 は、ハードディスクによる番組記録再生機能を内蔵させてある。なお、受信機 1 0 と受像機 5 は一体化されている場合もある。

図 2 は、本例の放送局 1, 2 の構成例を示す図である。本例では、映像コンテンツデータベース 1 0 1 と、オーディオコンテンツデータベース 1 0 2 と、公開鍵データベース 1 0 3 と、秘密鍵

データベース 104 と、データコンテンツデータベース 111 と、参照許可条件データベース 114 とが、データベースとして用意されている。公開鍵データベース 103 と、秘密鍵データベース 104 には、鍵発行サーバ 105 で生成された公開鍵及び秘密鍵をそれぞれ保存する。

映像コンテンツデータベース 101 とオーディオコンテンツデータベース 102 には、放送素材となる映像／オーディオ／データコンテンツを格納してある。映像コンテンツデータベース 101 から出力された映像コンテンツデータを、ビデオエンコーダ 106 で M P E G ビデオストリームパケットにエンコードし、多重化装置 108 に供給する。オーディオコンテンツデータベース 102 から出力されたオーディオストリームパケットを、オーディオエンコーダ 107 で M P E G オーディオストリームパケットにエンコードし、多重化装置 108 に供給する。

多重化装置 108 では、映像パケットとオーディオパケットと共に、データエンコーダ 109 から供給されるデータを多重化して、送出装置 110 に供給し、その多重化されたデータを放送データとして送出する。

データエンコーダ 109 では、データコンテンツデータベース 111 から供給されるデータコンテンツと公開鍵データベース 103 から供給される公開鍵のデータとを、M P E G データパケットに変換するエンコード処理を行い、処理された M P E G データパケットを、多重化装置 108 に供給する。

参照許可条件データベース 114 には、放送局に用意された各コンテンツに対して、その参照を許可する条件が登録してある。参照を許可する条件としては、例えば、放送局、コンテンツ中で参照を許可／禁止する部分、許可／禁止する提示方法、利用料金などがある。

この参照許可条件データベース 114 に格納されたデータと、
秘密鍵データベース 104 に保持された秘密鍵のデータは、署名
処理サーバ 113 に供給する。署名処理サーバ 113 は、署名を
依頼される側の放送局であるとき（後述する図 5 の例の放送局 1
5 ）、ネットワーク 3 を経由して受信したメタデータに署名を行い、
メタデータの送信元に送信する。署名を依頼する側（後述する
図 5 の例の放送局 2）から提示されたメタデータには、参照先コ
ンテンツ、参照位置、提示方法が記述されており、その内容が、
事前に設定して参照許可条件データベース 114 に格納された参
照許可条件と一致したとき、秘密鍵データベース 104 に保持さ
10 れた秘密鍵を使用して、メタデータに署名を行って、ネットワ
ーク 3 を介して依頼元に送信する。

署名依頼処理サーバ 112 は、署名を依頼する側の放送局であ
るとき（後述する図 5 の例の放送局 2）、署名を依頼される側の
15 放送局に対して、メタデータをネットワーク 3 に送信し、署名さ
れたメタデータをネットワーク 3 を介して受信して、その署名さ
れたメタデータを、データコンテンツデータベース 111 に格納
させる。

図 3 は、本例の受信機 10 の構成例を示す図である。受信機 1
20 0 は、セットトップボックス又は I R D（Integrated Receiver
Decoder）と称される構成ものである。衛星 4 からの放送波を受
信するアンテナ 11 は、受信機 10 内のチューナ部 12 に接続し
てあり、チューナ部 12 でこの受信機 10 の中央制御ユニット（
C P U）21 から指示された所定のチャンネルを受信する。チュ
25 ーナ部 12 で受信された信号（ベースバンド信号又は中間周波信
号）は、復調部 13 に供給して、伝送信号の変調方式に対応した
復調処理を行う。具体的には、例えば 8 相 P S K 復調，Q P S K
復調，6 4 Q A M 復調などの伝送信号に対応した復調方式での復

調が行われる。

5 復調部 13 で復調された受信信号は、ストリームデコーダ 14 に供給して、トランスポートストリームと称されるデジタルデータを抽出する。このとき、受信データに多重化されている各種データを分離する処理し、例えば番組を構成するコンテンツの映像データと音声データを分離し、さらにそのコンテンツに付加されて伝送された各種データについても分離する。このコンテンツに付加されて伝送されたデータの 1 つとして、メタデータと称されるものがある。このメタデータには、コンテンツを構成する番組の映像データの表示形態や、音声データの出力形態などを規定するデータが含まれる。また、後述する鍵データがメタデータに含まれる場合もある。

15 ストリームデコーダ 14 で抽出された映像データ及び音声データは、ここでは M P E G (Moving Picture Experts Group) 2 方式で圧縮符号化されたデジタルデータであり、この M P E G 2 方式の映像データ及び音声データのデコードを行う M P E G デコーダ 15 に供給して、M P E G 2 方式からのデコードを行う。デコードされた映像データは、合成部 16 で合成画像生成部 17 から供給される映像データの合成処理を必要により行った後、映像出力部 19 に供給し、接続された受像機 (図示せず) の映像処理回路に供給する。合成画像生成部 17 で生成させる合成用のデータについては、オンスクリーンディスプレイ (O S D) と称される文字、数字、記号などをメインの画像に重畳して表示させるためのデータの他に、子画面表示やマルチ画像表示などを行うためのデータなどの各種形態の表示が行えるようなデータを生成できるようにしてある。後述するメタデータに基づいて蓄積されたコンテンツの映像データと受信したコンテンツの映像データとを合成するためのデータについても、この合成画像生成部 17 で生成さ

れる。

また、MPEGデコーダ15でデコードされた音声データは、音声出力部18から受信機（又はステレオ再生装置などの音声処理装置）の音声処理回路に供給する。

- 5 なお、受信機10に接続された受信機などがデジタルデータを入力できる機器の場合には、映像出力部19や音声出力部18の出力は、デジタルデータのまま供給し、アナログ入力だけの機器が接続されている場合には、映像出力部19や音声出力部18でアナログ変換が必要である。また、受信機は受信機10に一体化
- 10 されている場合もある。

- ここまでの放送信号を受信して出力するまでのそれぞれの処理は、この受信機10が備える中央制御ユニット（CPU）21の制御で実行される。CPU21と受信機10内の各回路とは内部バスで接続されている。また、この内部バスを介して制御用のプ
- 15 ログラムなどが予め格納されたROM22と、ワークRAMであるRAM23とが接続してある。

- さらに本例の受信機10は、受信したコンテンツなどを記録するための大容量記憶手段としてのハードディスクドライブ（HDD）25を備え、そのHDD25でのデータの記録及び再生を、
- 20 内部バスに接続されたディスクコントローラ24の制御で実行するようにしてある。例えば、受信してストリームデコーダ14で抽出された所定のコンテンツの映像データ、音声データと、そのコンテンツのメタデータを、ディスクコントローラ24の制御でHDD25の所定のエリアに記録させる処理が行われる。そして
- 25 、記録されたデータは、ディスクコントローラ24の制御で読出されて、映像データや音声データについてはMPEGデコーダ15に供給して、デコードされた後、接続された受信機などに再生データとして供給させる。読出されたメタデータについては、C

P U 2 1 に供給し、映像データや音声データを処理する上で必要な制御処理を判断する。H D D 2 5 は、例えば数十Gバイト～数百Gバイトの記憶容量を有して、数十時間から数百時間分の映像データなどを記憶できる。

5 なお、H D D 2 5 の代わりに、例えば着脱自在な記録メディアを使用した記録手段を使用しても良い。

 そして本例においては、H D D 2 5 に記憶させるコンテンツのメタデータに鍵データが付加されている場合には、該当するコンテンツがH D D 2 5 に記録（蓄積）され続ける限りは、その鍵データについてそのままH D D 2 5 に記録させて保持させるようにしてある。H D D 2 5 に記録されたコンテンツのデータの読出しに、特に制限がない場合には、受信機10の操作手段（図示せず）のユーザの操作に基づいて、任意のときに再生処理が行われる。

15 また、H D D 2 5 に記録されたコンテンツ（以下コンテンツAとする）とは別のコンテンツ（以下コンテンツBとする）を受信機10が受信し、その受信したコンテンツBに含まれるメタデータで、H D D 2 5 に記録されたコンテンツAを参照することが指示されたときには、受信したコンテンツBに含まれるメタデータ
20 中の所定のデータを、H D D 2 5 に記録されたコンテンツAのメタデータに含まれる鍵データで照合し、照合を確認したときだけ、コンテンツAを参照した処理が行えるようにしてある。

 なお、このとき照合に使用する鍵データは、コンテンツAに対して放送局側で生成された秘密鍵（シークレットキー）データ及び公開鍵（パブリックキー）データの内の、公開鍵データであり
25 秘密鍵データについては公開されずに放送局内で保持される。この公開鍵と秘密鍵を使用した処理の詳細については後述する。

 次に、このコンテンツBがコンテンツAを参照するデータ処理

から見た受信機 10 の構成を図 4 に示す。受信機 10 内のチューナ部 12 で受信して復調部 13 及びデコーダ 14 で処理されたコンテンツのデータは、HDD 25 に蓄積させる場合には、HDD 25 内のコンテンツ格納部 25a に格納され、そのコンテンツのメタデータ及び公開鍵データについては、HDD 25 内のメタデータ格納部 25b に格納される。HDD 25 内のコンテンツ格納部 25a とメタデータ格納部 25b は、ディスクコントローラ 24 の制御で仮想的に記録エリアが分割されて設定されるものである。

そして、この受信機 10 でコンテンツ B を受信し、そのコンテンツ B のメタデータを CPU 21 内の制御部 21a が判断して、蓄積されたコンテンツ A を参照することが要求されている場合に、コンテンツ B のメタデータの内の一部のデータを、制御部 21a から CPU 21 内に構成される署名照合部 21b に送る。そして、この署名照合部 21b では、そのデータの電子署名の照合を、HDD 25 に蓄積されたコンテンツ A のメタデータに付加された公開鍵データを使用して行い、照合が確認されたとき、HDD 25 に蓄積されたコンテンツ A を読出して、MPEG デコーダ 15 でのデコードを行い、コンテンツ B のデータのデコードについても行う。そして、デコードされたコンテンツ A、B の映像データ及び音声データを、コンテンツ B のメタデータで指示された態様で、合成部 16 及び合成画像生成部 17 を使用して合成処理（又は選択処理）して、この受信機 10 から出力させる。

署名照合部 21b で電子署名の照合が確認できない場合には、MPEG デコーダ 15 でコンテンツ A のデコードを許可させず、コンテンツ B による画像や音声の出力時にコンテンツ A を参照できないように制限させる。

次に、このようなコンテンツ B によるコンテンツ A の参照処理

の流れを、図 5 のチャートを参照して説明する。図 5 は、放送システム全体から見た流れの図であり、ここではコンテンツ A を図 1 に示した放送局 1 が送出し、コンテンツ B を図 1 に示した放送局 2 が送出し、それぞれのコンテンツ A, B を受信機 10 で受信するものとする。

まず放送局 1 では、コンテンツ A を送出するに先立って、このコンテンツ A に対する秘密鍵データと公開鍵データの組を生成させ（ステップ S T 1 1）、コンテンツ A を放送する際に、そのとき生成された公開鍵データをメタデータに付加させる（ステップ S T 1 2）。受信機 10 では、このコンテンツ A を受信して、このコンテンツ A を受信機 10 内の HDD 25 に蓄積させるとき、メタデータに付加された公開鍵データについても蓄積させる（ステップ S T 1 3）。

その後、放送局 2 でコンテンツ A を参照するコンテンツ B を生成させたとき、放送局 2 は、ネットワーク 3 経由で放送局 1 に対して、コンテンツ B のメタデータを送り、電子署名を依頼する（ステップ S T 1 4）。このとき放送局 1 では、放送局 2 からの依頼を承諾するか否か、依頼の条件や内容などから判断する。この依頼に応じるか否かは、例えばライセンス条件やコンテンツ A の利用料金などを判断して決める。

そして、依頼に応じるとき、コンテンツ B のメタデータの一部、又はコンテンツ B のメタデータに関連するデータに、コンテンツ A に対して生成させた秘密鍵データを使用して電子署名する（ステップ S T 1 5）。そして、その電子署名されたメタデータを放送局 1 から、ネットワーク 3 経由で放送局 2 に伝送する（ステップ S T 1 6）。

この電子署名されたメタデータを放送局 2 が受信した後は、その受信した電子署名されたメタデータをコンテンツ B に付加し

て（厳密にはコンテンツ B のデータ + コンテンツ B の原メタデータ + 電子署名データ）、放送開始時間になるとコンテンツ B の送信を行う（ステップ S T 1 7）。

5 そして、この放送されたコンテンツ B を受信機 1 0 が受信し、
このコンテンツ B のメタデータでコンテンツ A を参照することが
指示されていることを受信機 1 0 内の C P U 2 1 が判断すると、
上記電子署名されたメタデータを、受信機 1 0 内に蓄積されたコ
ンテンツ A の公開鍵データを使用して復号化して復号化データを
10 生成する。一方、コンテンツ B のメタデータも送信側が電子署名
で使用した同じ所定のアルゴリズムでデータ変換を行い、変換デ
ータを生成する。そして、上記復号化データと上記変換データと
の照合処理を行う。そして、この照合に成功したか否か判断し、
照合に成功した場合だけ、コンテンツ B のメタデータで指示され
た方法で、蓄積されたコンテンツ A と受信したコンテンツ B とを
15 合成して、受信機 1 0 から出力させ、接続された受像機 5 で視聴
させる（ステップ S T 1 8）。なお、コンテンツ B を受信すると
同時に、コンテンツ A とコンテンツ B を合成させたデータの出力
を行うのではなく、コンテンツ B についても受信機 1 0 内の H D
D 2 5 に蓄積させて、その蓄積されたコンテンツ B を出力させる
20 とき、コンテンツ A を参照して合成などを行うようにしても良い
。

図 6 は、図 5 のフローチャートで示した処理を、データの流れ
から見た図である。図 6 の中のステップ数は、図 5 に一致させて
ある。コンテンツ A を放送した放送局 1 では、秘密鍵データと公
25 開鍵データとを生成させて、コンテンツ A を放送する際には、コ
ンテンツ A のデータに公開鍵データが付加されている。コンテン
ツ A を参照するコンテンツ B を放送する放送局 2 では、放送局 1
との間で、メタデータの署名の依頼と、その依頼したメタデータ

の返送が行われる。そして放送局 2 は、この署名されたメタデータが付加されたコンテンツ B を放送する。

ここで、秘密鍵データと公開鍵データとを使用した電子署名の処理例について、図 7 を参照して説明する。まず、電子署名したいコンテンツ B のメタデータがある場合、そのメタデータのメッセージダイジェストを作成する（ステップ S T 2 1）。なお、このときのメタデータには、コンテンツ A の参照命令を少なくとも含むものである。また、ここでのメッセージダイジェストとは、元のデータの特徴を表す固定長（例えば 1 2 8 ビット程度）のビットパターンで、予め決められた所定のアルゴリズムで生成される。このメッセージダイジェストは、異なるデータに対して同じメッセージダイジェストが生成される確率は極めて低く、メッセージダイジェストが変わらないように元のデータ（メタデータ）を改変することは実質上不可能である。

このメッセージダイジェストの生成は、例えば放送局 2 側で行う（放送局 1 側で行っても良い）。そして、そのメッセージダイジェストを放送局 1 に送って、放送局 1 に保持された秘密鍵データを使用して暗号化して、電子署名されたデータとする（ステップ S T 2 2）。この際に使用される公開鍵暗号系としては、R S A 方式などが知られている。そして放送局 2 内では、この電子署名されたメッセージダイジェストのデータを、コンテンツ B のメタデータに付加して放送する（ステップ S T 2 3）。

そして、コンテンツ B を受信した受信機内では、そのコンテンツ B のメタデータに付加された電子署名されたメッセージダイジェストのデータを抽出し、そのデータを受信機内で保持されたコンテンツ A の公開鍵データで復号する（ステップ S T 2 4）。また受信機内で、コンテンツ B のメタデータから、メッセージダイジェストを生成させる（ステップ S T 2 5）。このときには、ス

5 テップ S T 2 1 でメッセージダイジェストを生成させた際と同じ
アルゴリズムを使用して生成させる。そして、生成されたメッ
セージダイジェストと復号されたデータとを受信機内で比較し（ス
テップ S T 2 6）、一致したとき、受信機内で電子署名を確認し
たものと判断する。

10 次に、このような処理で実行されるコンテンツ B によるコン
テンツ A の参照処理の例を説明する。図 8 は、コンテンツ B がコン
テンツ A の番組紹介を行うコンテンツである例である。ステップ
S T 3 1 でコンテンツ A が、メタ（1）に記述された公開鍵と共
15 に放送されて、そのデータが受信機で蓄積された後、ステップ
S T 3 2 でそのコンテンツ A を参照するコンテンツ B が送信された
とき、受信機に接続された受像機の画面では、メタ（2）の記述
に従い、コンテンツ A の映像データ A V（1）の主要な場面の画
像などが縮小されて表示され、コンテンツ B の映像データ A V（
20 2）による番組の紹介者などの画像などが合成されて表示される。
ここでメタ（2）には、参照される A V（1）および参照範囲
（開始／終了位置）、A V（1）および A V（2）の画面上での
表示位置／縮小比率／タイミングに関する情報が、これらの記述
に対する電子署名と共に記述される。また、コンテンツ A の番組
25 の内容をメタ（2）中にテキストデータとして記述しておき、そ
の内容を文字などで紹介する画像についても、コンテンツ B のデ
ータであるメタ（2）の指示（すなわち表示位置／タイミング、
表示書式など）に基づいて受信機内で生成されて、同時に表示さ
れるようにしても良い。また、音声についても、コンテンツ A の
番組の音声の一部に、コンテンツ B による音声を合成させても良
い。

 この図 8 に示した例でのメタデータの例を示すと、以下のよう
になる。

```

<メタデータ>
.....
<参照 i d = " R 1 " >
  <参照先>
5    <コンテンツ>A V 1</コンテンツ>
    <開始位置>t1</開始位置>
    <終了位置>t2</終了位置>
  </参照先>
  <提示形態>
10  <子画面表示>
    <参照コンテンツ表示位置>(XA, YA)</参照コンテンツ表示位置>
    <参照コンテンツ縮小率>50%</参照コンテンツ縮小率>
    <オリジナルコンテンツ表示位置>(XB, YB)</オリジナルコンテンツ表示位置>
    <オリジナルコンテンツ縮小率>50%</オリジナルコンテンツ縮小率>
15  <表示タイミング>t3</表示タイミング>
    </子画面表示>
    </提示形態>
  </参照>
  .....
20  <署名>
    <Signature xmlns="http://www.w3c.org/2000/09/xmldsig#">
      <SignedInfo>
        .....
        <ReferenceURI= "#R1" >....</Reference>
25  </SignedInfo>
    </Signature>
  </署名>
</メタデータ>

```

この例のメタデータの署名部分は、XML-Signature の仕様に従った記述である。この例では、署名の対象が<参照 id = “R 1”>から始まる部分であることが示されている。また、子画面表示の表示形態として、1 画面中での表示位置 (X_A, Y_A) 及び (X_B, Y_B) (図 8 参照) と、表示される縮小率が指定されて、図 8 に示したような子画面表示が行われる状態を指定している。

図 9 は、この図 8 の例による端末側での処理例を示したフローチャートである。このフローチャートに従って説明すると、まずステップ S 1 1 において、復調部 1 3 及びストリームデコーダ 1 4 にて、入力ストリームデータを、コンテンツとメタデータに分離する。

次にステップ S 1 2 において、制御部 2 1 a にてメタデータをパースし、「参照」要素及び対応する「署名」要素の内容を抽出する。そしてステップ S 1 3 において、署名照合部 2 1 b にて、「参照」要素中の「コンテンツ」要素の内容を元に、事前に蓄積しておいたコンテンツ A の公開鍵をメタデータ格納部 2 5 b から取り出す。

そしてステップ S 1 4 において、署名照合部 2 1 b にて、取り出した公開鍵を用いて、「参照」／「署名」の内容を照合する。

このとき、ステップ S 1 5 で、照合に成功したか否か判断し、照合に成功しないときには、ステップ S 1 6 に移り、処理を中断させる。また、照合に成功した場合には、ステップ S 1 7 に移り、デコーダ 1 5, 合成部 1 6, 合成画像生成部 1 7 において、制御部 2 1 a と署名照合部 2 1 b の指示に基づき、ストリームデコーダ 1 4 から出力されるストリームである、コンテンツ B のデコード及び表示を開始させる。

その後、ステップ S 1 8 に移り、時刻 t₀ まで待機する。さら

にステップ S 1 9 に移り、デコーダ 1 5 において、署名照合部 2 1 b の指示に基づき、メタデータ格納部 2 5 a に格納されているコンテンツ A について、タイミング t_1 からタイミング t_2 までのデコードを開始する。このとき同時に、制御部 2 1 a の指示に基づき合成部 1 6 及び合成画像生成部 1 7 でのコンテンツ A 及び B の合成及び表示を開始させる。

ここでは番組紹介を行う例としたが、他の参照処理を行うようにしても良い。例えば、コンテンツ A としてサッカーゲームなどのスポーツ中継の番組とし、コンテンツ B として、そのスポーツ中継のハイライトシーンなどの一部の場面だけを紹介するスポーツニュース番組としてのコンテンツとし、コンテンツ B を視聴させるとき、コンテンツ A として蓄積された画像の中のハイライトシーンを順に紹介するような画像や音声を出力させても良い。

また、映画やドラマなどのコンテンツ（コンテンツ A）を語学学習用の教材として参照するような場合に、コンテンツ B でその参照するようなデータを送り、図 8 に示したような番組紹介の代わりに、コンテンツ A の映像や音声に何らかの編集処理を施して、その映像や音声の出力和同時にセリフの原語表示、翻訳表示などを文字で行ったり、翻訳された音声を出力させるようにしても良い。

このように本例の処理を行うことで、既に送られて蓄積されたコンテンツ A を参照するコンテンツ B の視聴が可能になるが、いずれの場合でも、受信機側では公開鍵データを使用して一致が確認できた場合にだけ、このような参照処理を行うので、コンテンツ A を送出させた放送局側が秘密鍵データを外部に漏らさない限りは、コンテンツ A を送出させた放送局で承認がされない限り、コンテンツ A を参照する視聴が行えないので、著作権などを侵害するような形での他のコンテンツの参照を効果的に防止できる。

また、図 10 は、コンテンツ B によるコンテンツ A の参照処理として、コンテンツ A の映像及び音声の一部を、コンテンツ B の映像及び音声に置き替える場合の例である。即ち、図 10 A に示すように、コンテンツ A による番組として、シーン 1, シーン 2, シーン 3 などの場面の变化時に、特定のコマーシャル CM 1, CM 2, CM 3 ……を入れてあるものとする。このとき、コンテンツ B として、図 10 B に示すように、このコンテンツ A のコマーシャル CM 1, CM 2, CM 3 ……を置き替えるコマーシャル CM 1 1, CM 1 2, CM 1 3 ……の映像及び音声を送る。この場合には、コンテンツ B のデータについても、受信機内の HDD に蓄積させる。このデータにはコンテンツ A における CM 1, CM 2, CM 3 ……の開始／終了位置、コンテンツ B における CM 1 1, CM 1 2, CM 1 3 ……の開始／終了位置、および CM 1 と CM 1 1、CM 2 と CM 1 2、……を置き替えることを指示するコマンドが、これらの記述に対する電子署名と共に記述される。そして、コンテンツ B を受信した後にコンテンツ A の番組を視聴するときには、図 10 C に示すように、HDD 中に格納されたデータの指示に従って、コマーシャル CM 1, CM 2, CM 3 ……をコマーシャル CM 1 1, CM 1 2, CM 1 3 ……に置き替えて出力させて視聴させる。

この図 10 に示した例でのメタデータの例を示すと、以下のようになる。

<メタデータ>

……

<参照 id = “R1” >

<参照先>

<コンテンツ>コンテンツ A </コンテンツ>

<開始位置> s₁ </開始位置>

<終了位置>e₁</終了位置>
 </参照先>
 <提示形態>
 <置換>
 5 <コンテンツ>コンテンツ A</コンテンツ>
 <開始位置>s₁₁</開始位置>
 <終了位置>e₁₁</終了位置>
 </置換>
 </提示形態>
 10 </参照>
 <参照 id = "R2" ></参照> (→CM2,CM12に関する記述)
 <参照 id = "R3" ></参照> (→CM3,CM13に関する記述)

 <署名>
 15 <Signature xmlns="http://www.w3c.org/2000/09/xmldsig#">
 <SignedInfo>

 <ReferenceURI= "#R1" >....</Reference>
 </SignedInfo>
 20 <Signature>
 </署名>
 <署名>.....</署名> (→ <参照id= "R2" > 部分の署名)
 <署名>.....</署名> (→ <参照id= "R3" > 部分の署名)
 </メタデータ>
 25 このメタデータの例の内の括弧書きの部分は、メタデータの内容を説明したものである。この例のメタデータの署名部分についても、XML-Signature の仕様に従った記述であり、<ReferenceURI= "#R1" > との記述は、署名の対象が <参照 id = "R1

” > から始まる部分であることを表している。

この例では、〈参照先〉として、コンテンツ A の CM 1 の開始位置 s_1 と終了位置 e_1 が記述されている。また、提示形態が〈置換〉であるコンテンツ B の CM 1 1 の開始位置 s_{11} と終了位置 e_{11} が記述され、コンテンツ A の CM 1 が、コンテンツ B の CM 1 1 に置換されることを表している。

図 1 1 は、この図 1 0 の例による端末側での処理例を示したフローチャートである。このフローチャートに従って説明すると、まずステップ S 2 1 において、復調部 1 3 及びストリームデコーダ 1 4 にて、入力ストリームデータを、コンテンツとメタデータに分離し、ストリームデータをコンテンツ格納部 2 5 a に格納させ、メタデータをメタデータ格納部 2 5 b に格納させる。

次に、ステップ S 2 2 において、制御部 2 1 a にて、メタデータをパースし、各「参照」要素および対応する「署名」要素の内容を抽出する。そしてステップ S 2 3 で、署名照合部 2 1 b にて、「参照」要素中の「コンテンツ」要素の内容を元に、事前に蓄積しておいたコンテンツ A の公開鍵をメタデータ格納部 2 5 b から取り出す。

この公開鍵が取り出されると、ステップ S 2 4 に移って、署名照合部 2 1 b にて、取り出した公開鍵を用いて、各「参照」／「署名」の内容を照合する。そして、ステップ S 2 5 で、この照合に成功したか否か判断する。照合に失敗したときには、ステップ S 2 6 に移って、処理を中断する。

照合に成功した場合には、ステップ S 2 7 に移り、デコーダ 1 5，合成部 1 6，合成画像生成部 1 7 において、制御部 2 1 a と署名照合部 2 1 b の指示に基づき、コンテンツ格納部 2 5 a に格納されたコンテンツ A のデコード及び表示を開始させる。

その後、ステップ S 2 8 に移り、全ての処理が完了したか否か

判断し、全ての処理が終了したと判断したとき、ステップ S 2 9 に移り、コンテンツ A の残りを再生して終了する。

5 ステップ S 2 8 で、全ての処理が完了してないと判断したとき、ステップ S 3 0 に移る。ここで、残りの参照のうち開始位置が最も早いものの開始位置を s_i 、終了位置を e_i とするとき（図 1 0 A 参照）、コンテンツ A の再生が開始位置 s_i に差し掛かるまで待つ。

10 そしてステップ S 3 1 に移り、デコーダ 1 5，合成部 1 6，合成画像生成部 1 7 において、制御部 2 1 a と署名照合部 2 1 b の指示に基づき、コンテンツ A の再生を中断し、代わりに「置換」要素の内容に従って、コンテンツ B の CM 1 1 部分のデコードとそのデコードされたデータの表示を、開始位置 s_i 。（図 1 0 B 参照）から行われる。

15 その後、さらにステップ S 3 2 に移り、デコーダ 1 5，合成部 1 6，合成画像生成部 1 7 において、制御部 2 1 a と署名照合部 2 1 b の指示に基づき、終了位置 e_i 。（図 1 0 B 参照）でコンテンツ B の再生を終了し、位置 e_i からコンテンツ A の再生を再開させる。

20 この図 1 0，図 1 1 に示すように処理することで、例えば最初にコンテンツ A に含まれたコマーシャルで宣伝する内容に時期的な有効期限などがある場合、その期限が切れた時点で、新たなコマーシャルをコンテンツ B として送ることで、ユーザ側では常に最新のコマーシャルを視聴できるようになる。この場合、最初にコンテンツ A に入っていたコマーシャルと差し替えることが承認
25 されない限り、別のコマーシャルに差し替えられることはないの
 で、そのコマーシャルを流しているスポンサーの権利を侵害する
 ような形で差し替えられることはない。

 なお、ここまでの説明では、各コンテンツの鍵データは、放送

局が保持するようにしたが、放送局とは別の鍵管理サーバ（鍵管理会社）をネットワーク上に設けて、その鍵管理サーバが秘密鍵データや公開鍵データを管理するようにしても良い。図 1 2 はその場合のシステム構成例を示した図であり、放送局 1, 2 に接続されたネットワーク 3 には、鍵管理サーバ 6 が接続されている。

図 1 3 は、放送局 1, 2 と鍵管理サーバ 6 とを別にした場合の、放送局 1, 2 の構成例を示した図である。

この例では、映像コンテンツデータベース 1 0 1 と、オーディオコンテンツデータベース 1 0 2 と、公開鍵データベース 1 0 3 と、データコンテンツデータベース 1 1 1 とが、データベースとして用意されている。公開鍵データベース 1 0 3 には、公開鍵を保存する。

映像コンテンツデータベース 1 0 1 とオーディオコンテンツデータベース 1 0 2 には、放送素材となる映像／オーディオ／データコンテンツを格納してある。映像コンテンツデータベース 1 0 1 から出力された映像コンテンツデータを、ビデオエンコーダ 1 0 6 で M P E G ビデオストリームパケットにエンコードし、多重化装置 1 0 8 に供給する。オーディオコンテンツデータベース 1 0 2 から出力されたオーディオストリームパケットを、オーディオエンコーダ 1 0 7 で M P E G オーディオストリームパケットにエンコードし、多重化装置 1 0 8 に供給する。

多重化装置 1 0 8 では、映像パケットとオーディオパケットとに、データエンコーダ 1 0 9 から供給されるデータを多重化して、送出装置 1 1 0 に供給し、その多重化されたデータを放送データとして送出する。

データエンコーダ 1 0 9 では、データコンテンツデータベース 1 1 1 から供給されるデータコンテンツと公開鍵データベース 1 0 3 から供給される公開鍵のデータとを、M P E G データパケッ

トに変換するエンコード処理を行い、処理されたMPEGデータ
パケットを、多重化装置108に供給する。

署名依頼処理サーバ112は、署名を依頼する側の放送局であ
るとき、署名を依頼される側に対して、メタデータをネットワー
ク3に送信し、署名されたメタデータをネットワーク3を介して
5 受信して、その署名されたメタデータを、データコンテンツデー
タベース111に格納させる。

図14は、鍵管理サーバ6の構成例を示した図である。鍵管理
サーバ6は、データベースとして、公開鍵データベース201と
10 、秘密鍵データベース202と、参照許可条件データベース20
3とを備える。公開鍵データベース201と、秘密鍵データベー
ス202が格納する公開鍵及び秘密鍵は、鍵発行サーバ204が
生成させたものである。署名処理サーバ205は、ネットワーク
3を介してメタデータに署名依頼があるとき、参照許可条件デー
タベース203に格納された参照条件を満たすとき、秘密鍵デー
15 タベース202が格納した秘密鍵を使用して、メタデータに署名
して、依頼した放送局側にネットワーク3を介して送信する。

図15は、この鍵管理サーバ6を使用した場合のコンテンツA
、Bの送出处理例を示した図である。まず、コンテンツAを送出
20 する放送局1では、そのコンテンツAを他のコンテンツが利用す
る際のライセンス条件を、鍵管理サーバ6に登録させる（ステッ
プST41）。そして、鍵管理サーバ6では、コンテンツAに対
する秘密鍵データと公開鍵データを生成させ（ステップST42
）、公開鍵データだけを放送局1に送る（ステップST43）。
25 秘密鍵データについては、鍵管理サーバ6内で保持させておく。

ここまでの処理が行われた後に、放送局1はコンテンツAに公
開鍵データをメタデータを付加して送信する（ステップST44
）。受信機10では、このコンテンツAを受信して、このコンテ

ンツ A を受信機 10 内の HDD 25 に蓄積させるとき、メタデータに付加された公開鍵データについても蓄積させる（ステップ S T 45）。

5 その後、放送局 2 でコンテンツ A を参照するコンテンツ B を生成させたとき、放送局 2 は、ネットワーク 3 経由で鍵管理サーバ 6 に対して、コンテンツ B のメタデータを送り、電子署名を依頼する（ステップ S T 46）。このとき鍵管理サーバ 6 では、コンテンツ A に対して登録されたライセンス条件のデータを、放送局 2 に送り（ステップ S T 47）、そのライセンス条件に同意する
10 データが鍵管理サーバ 6 に送られたとき（ステップ S T 48）、コンテンツ B のメタデータから生成されたメッセージダイジェストに、コンテンツ A に対して生成させた秘密鍵データを使用して電子署名する（ステップ S T 49）。そして、その電子署名されたメタデータを鍵管理サーバ 6 から、ネットワーク 3 経由で放送
15 局 2 に伝送する（ステップ S T 50）。

 この電子署名されたメタデータを放送局 2 が受信した後は、その受信した電子署名されたデータをコンテンツ B のメタデータに付加して、放送開始時間になるとコンテンツ B の送信を行う（ステップ S T 51）。

20 そして、この放送されたコンテンツ B を受信機 10 が受信し、このコンテンツ B のメタデータでコンテンツ A を参照することが指示されていることを受信機 10 内の CPU 21 が判断すると、コンテンツ B のメタデータの一部を、受信機 10 内に蓄積されたコンテンツ A の公開鍵データを使用して照合し、照合に成功した
25 か否か判断し、照合に成功した場合だけ、コンテンツ B のメタデータで指示された方法で、蓄積されたコンテンツ A と受信したコンテンツ B とを合成して、受信機 10 から出力させ、接続された受信機 5 で視聴させる（ステップ S T 52）。

図 1 6 は、図 1 5 のフローチャートで示した処理を、データの
流れから見た図である。図 1 6 の中のステップ数は、図 1 5 に一
致させてある。コンテンツ A を放送した放送局 1 とは別の鍵管理
サーバ 6 では、秘密鍵データと公開鍵データとを生成させて保持
5 させてある。そして、放送局 1 がコンテンツ A を放送する際には
、コンテンツ A のデータに公開鍵データが付加されている。コン
テンツ A を参照するコンテンツ B を放送する放送局 2 では、鍵管
理サーバ 6 との間で、メタデータの署名の依頼と、その依頼した
メタデータの返送が行われる。そして放送局 2 は、この署名され
10 たメタデータが付加されたコンテンツ B を放送する。

このように放送局とは別の鍵管理サーバを設けたことでも、上
述した図 1 ～図 1 1 に示した処理と同様の処理が可能になる。

なお、上述した実施の形態では、コンテンツ A を配信する第 1
の放送局 1 とコンテンツ B を配信する第 2 の放送局 2 とが別の放
15 送局である例としたが、コンテンツ A, B を配信する放送局が同
じであっても良い。なお、ここでの放送局とは、コンテンツを送
信させるいわゆる送信所として示したが、放送局ではコンテンツ
の配信や管理だけを行って、そのコンテンツの送信については、
別の送信所から行う構成であっても良い。

また、上述した実施の形態では、衛星放送を利用した放送シス
テムに適用した例としたが、他の伝送路による放送システムにも
適用可能である。この場合、予め規定された伝送チャンネルで放
送を行うテレビジョン放送やラジオ放送のような一般的な意味で
20 の放送だけでなく、無線又は有線の伝送路を使用して不特定多数
のユーザにコンテンツを配信するサービスであれば適用可能であ
り、例えばいわゆるインターネット放送のような、何らかのネッ
トワークで接続された不特定多数のユーザ（或いは予め契約され
た複数のユーザ）の端末（受信機）に対して、サーバ（放送局）
25

側から各種コンテンツを配信させる際にも、本発明を適用することが可能である。

5 また、上述した実施の形態の説明では、後から送信されるコンテンツが参照する過去のコンテンツは、1つのコンテンツだけとしたが、蓄積された複数のコンテンツを参照するような場合にも適用可能である。

10 また、上述した実施の形態では、放送される各コンテンツのスクランブル処理については何も説明しなかったが、何らかのスクランブル処理を施して放送して、契約された特定のユーザの受信機だけが受信できるようにしても良い。この場合、元のコンテンツAを参照するコンテンツBを視聴する際にだけ、スクランブルがかかるようにして、契約（課金）されたユーザだけがコンテンツBによる視聴ができるようにしても良い。逆に、コンテンツAに対してスクランブルを施し、コンテンツBによる参照時（例えば番組紹介など）にはスクランブルがかからないようにして、課金処理を行ったユーザだけが、コンテンツAを完全に視聴できるようにしても良い。

20 また、上述した実施の形態では、放送信号として放送局から受信端末に伝送する場合について説明したが、放送以外の形態でストリームデータを伝送する場合にも適用可能である。

25 また、上述した実施の形態では、放送局及び受信機のいずれも、データ格納手段やエンコーダ、デコーダなどを専用の回路で構成させるようにしたが、例えば同様の処理を実行するソフトウェアを、コンピュータ装置などのデータ処理装置に組み込んで、放送局又は受信機として機能するようにしても良い。この場合、ソフトウェアは、ディスク、テープ、メモ리카ードなどの媒体に記憶させて配付する他に、インターネットなどの伝送媒体を使用して配付するようにしても良い。

産業上の利用可能性

本発明にかかる情報処理方法、情報処理装置、電子機器及び媒体によると、最初に送ったコンテンツの管理者に参照することが許可された場合にだけ、正しい署名が行われた所定データが別のコンテンツに付加されるので、最初に送信されたコンテンツを蓄積した各受信者側の設備では、そのコンテンツを参照しても良いと許可されたコンテンツを受信したときだけ、自動的に別のコンテンツが参照するようになる。従って、過去のコンテンツの製作者や放送業者の権利を守った上で、随時その過去のコンテンツを参照した新たなコンテンツを制作して配信できるようになる。

この場合、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツの一部を利用した別のコンテンツを作成して視聴させることが良好にできるようになる。

また、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツの一部の画像や音声などを最新のデータに置き替えて視聴させることができるようになる。

さらに、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツのハイライトシーンだけを表示させるようなことが可能になる。

請 求 の 範 囲

1. ネットワークを介して情報の授受を行う情報処理装置において、

5 上記第1のコンテンツに対して、秘密鍵と公開鍵を生成させて管理する鍵管理手段と、

 上記鍵管理手段で管理する公開鍵を付加して、上記第1のコンテンツを送信する第1の送信手段と、

10 上記第2のコンテンツに付加される所定データに対して、上記鍵管理手段が管理する秘密鍵での電子署名を要求し、その電子署名された所定データが付加された上記第2のコンテンツを送信する第2の送信手段とを備えたこと

 を特徴とする情報処理装置。

2. 上記鍵管理手段は、上記第2の送信手段からの電子署名要求時に、上記第2のコンテンツによる第1のコンテンツの参照が、第1のコンテンツの所定の権利を侵害しないと判断したとき
15 だけ、上記所定データへの電子署名を実行すること

 を特徴とする請求項1記載の情報処理装置。

3. ネットワークを介して情報の授受を行う情報処理装置において、

20 第1のコンテンツと、第1のコンテンツに関連する所定データとを、第2のコンテンツに適用される秘密鍵を用いて上記所定データに電子署名を行った電子署名データに組み合わせて送信する第1の送信手段を備えること

 を特徴とする情報処理装置。

4. 上記電子署名データを取得する電子署名データ取得手段を有すること
25

 を特徴とする請求項3記載の情報処理装置。

5. 上記秘密鍵を使用して電子署名が行われる上記所定データは

- 、上記第 2 のコンテンツの参照命令を含むこと
を特徴とする請求項 3 記載の情報処理装置。
6. 上記所定データは、第 1 のコンテンツに対する挿入開始位置
情報、挿入終了位置情報及び対応する第 2 のコンテンツの参照
5 開始位置情報、参照終了位置情報を有すること
を特徴とする請求項 5 記載の情報処理装置。
7. コンテンツデータを受信する受信手段と、
上記受信手段が受信したコンテンツを蓄積するコンテンツ蓄
積手段と、
10 上記コンテンツ蓄積手段に蓄積された第 1 のコンテンツに付
加された鍵データを使用して、上記受信手段が受信した第 2 の
コンテンツに付加された所定データの電子署名を照合する照合
手段と、
上記照合手段での照合が成功したとき、上記コンテンツ蓄積
15 手段に蓄積された第 1 のコンテンツを、上記第 2 のコンテンツ
での指示に基づいて加工するコンテンツ加工手段と、
上記コンテンツ加工手段で加工されたコンテンツを出力する
コンテンツ出力手段とを備えた
電子機器。
- 20 8. 上記コンテンツ加工手段での加工は、上記第 1 のコンテンツ
による画像又は音声と上記第 2 のコンテンツによる画像又は音
声を合成する処理であること
を特徴とする請求項 7 記載の電子機器。
9. 上記コンテンツ加工手段での加工は、上記第 1 のコンテンツ
25 による画像又は音声の一部を、上記第 2 のコンテンツによる画
像又は音声に置き替える処理であること
を特徴とする請求項 7 記載の電子機器。
10. 上記コンテンツ加工手段での加工は、上記第 1 のコンテンツ

による画像又は音声を、第 2 のコンテンツによる指示で編集する処理であること

を特徴とする請求項 7 記載の電子機器。

- 5 11. ネットワークを介して情報の授受を行い、それら情報を記録及び／又は再生する電子機器において、

第 1 のコンテンツと、上記第 1 のコンテンツに関連する第 1 の所定データと、第 2 のコンテンツに適用される秘密鍵を上記第 1 の所定データに用い生成された電子署名データとの組み合わせデータを受信する第 1 の受信手段を有すること

- 10 を特徴とする電子機器。

12. 上記秘密鍵を使用して電子署名が行われる上記第 1 の所定データは、第 2 のコンテンツの参照命令を含むこと

を特徴とする請求項 11 記載の電子機器。

- 15 13. 上記第 1 の所定データは、第 1 のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第 2 のコンテンツの参照開始位置情報、参照終了位置情報を有すること

を特徴とする請求項 12 記載の電子機器。

14. 第 2 のコンテンツと上記秘密鍵に対応する公開鍵とを受信する第 2 の受信手段と、

- 20 受信された上記第 2 のコンテンツと上記公開鍵を記憶する記憶手段とを有すること

を特徴とする請求項 11 記載の電子機器。

15. 上記電子署名データを上記公開鍵を用い復号化し、復号化データを生成する復号化手段と、

- 25 上記第 1 の所定データを所定のアルゴリズムに基づいて第 2 の所定データに変換するデータ変換手段と、

上記復号化手段により生成された上記復号化データと、上記データ変換手段により変換された上記第 2 の所定データとを照

合する照合手段とを有すること

を特徴とする請求項 1 4 記載の電子機器。

- 5 16. 上記照合手段の照合結果が一致した場合、上記第 1 の所定データに基づき上記記憶手段に記憶された第 2 のコンテンツを所定のタイミングで参照する参照手段とを有すること

を特徴とする請求項 1 5 記載の電子機器。

17. 第 1 のコンテンツと、この第 1 のコンテンツを参照する第 2 のコンテンツを処理する情報処理方法において、

10 上記第 1 のコンテンツに対して、秘密鍵と公開鍵を生成させ、

上記生成された公開鍵を付加して、上記第 1 のコンテンツを送信し、

上記第 2 のコンテンツに付加される所定データに対して、上記秘密鍵での電子署名を要求し、

- 15 上記電子署名された所定データが付加された上記第 2 のコンテンツを送信すること

を特徴とする情報処理方法。

18. 送信される上記第 1 のコンテンツを受信して蓄積した状態で、送信される上記第 2 のコンテンツを受信した場合に、蓄積された第 1 のコンテンツに付加された公開鍵を使用して、上記所
20 定データの電子署名を照合し、

その照合に成功したとき、受信した上記第 2 のコンテンツの指示に基づいて、上記蓄積された第 1 のコンテンツに所定の加工を施して出力すること

- 25 上記を特徴とする請求項 1 7 記載の情報処理方法。

19. ネットワークを介して情報の授受を行う情報処理方法において、

第 1 のコンテンツと、第 1 のコンテンツに関連する所定デー

タとを送信する場合に、

上記第 1 のコンテンツとは別の第 2 のコンテンツに適用される秘密鍵を用いて、上記所定データに電子署名を行い、

5 その電子署名された電子署名データを上記所定データに組み合わせて送信する

を特徴とする情報処理方法。

20. 上記秘密鍵を用いた電子署名を、上記第 2 のコンテンツ又は上記秘密鍵を管理する側に依頼し、その依頼に基づいて得られた電子署名データを、上記所定データに組み合わせること

10 を特徴とする請求項 19 記載の情報処理方法。

21. 上記秘密鍵を使用して電子署名が行われる上記所定データは、上記第 2 のコンテンツの参照命令を含むこと

を特徴とする請求項 19 記載の情報処理方法。

22. 上記所定データは、第 1 のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第 2 のコンテンツの参照開始位置情報、参照終了位置情報を有すること

15 を特徴とする請求項 21 記載の情報処理方法。

23. ネットワークを介して情報の授受を行い、それら情報を記録及び／又は再生する情報処理方法において、

20 第 1 のコンテンツを記録するとき、上記第 1 のコンテンツに関連する第 1 の所定データと、既に記録された第 2 のコンテンツに適用される秘密鍵を上記第 1 の所定データに用い生成された電子署名データとを記録すること

を特徴とする情報処理方法。

25 24. 上記秘密鍵を使用して電子署名が行われる上記第 1 の所定データは、第 2 のコンテンツの参照命令を含むこと

を特徴とする請求項 23 記載の情報処理方法。

25. 上記第 1 の所定データは、第 1 のコンテンツに対する挿入開

始位置情報、挿入終了位置情報及び対応する第 2 のコンテンツ
の参照開始位置情報、参照終了位置情報を有すること
を特徴とする請求項 2 4 記載の情報処理方法。

5 26. 第 2 のコンテンツと上記秘密鍵に対応する公開鍵とを受信し
たとき、受信された上記第 2 のコンテンツと上記公開鍵を記録
すること

を特徴とする請求項 2 3 記載の情報処理方法。

 27. 上記電子署名データを上記公開鍵を用い復号化し、復号化デ
ータを生成し、
10 上記第 1 の所定データを所定のアルゴリズムに基づいて第 2
の所定データに変換し、
 上記復号化データと上記第 2 の所定データとを照合すること

を特徴とする請求項 2 6 記載の情報処理方法。

15 28. 上記照合の結果が一致した場合、上記第 1 の所定データに基
づき、既に記録された第 2 のコンテンツを所定のタイミングで
参照すること

を特徴とする請求項 2 7 記載の情報処理方法。

 29. 第 1 のコンテンツと、この第 1 のコンテンツを参照する第 2
20 のコンテンツを処理する情報処理を実行するプログラムを格納
又は伝送する媒体において、

 上記第 1 のコンテンツに対して、秘密鍵と公開鍵を生成させ
、

 上記生成された公開鍵を付加して、上記第 1 のコンテンツを
25 送信し、

 上記第 2 のコンテンツに付加される所定データに対して、上
記秘密鍵での電子署名を要求し、

 上記電子署名された所定データが付加された上記第 2 のコン

テンツを送信する処理を行う

ことを特徴とするプログラムを格納又は伝送する
媒体。

30. 上記プログラムは、さらに、

5 送信される上記第 1 のコンテンツを受信して蓄積した状態で
、送信される上記第 2 のコンテンツを受信した場合に、蓄積され
た第 1 のコンテンツに付加された公開鍵を使用して、上記所
定データの電子署名を照合し、

10 その照合に成功したとき、受信した上記第 2 のコンテンツの
指示に基づいて、上記蓄積された第 1 のコンテンツに所定の加
工を施して出力すること

を特徴とする請求項 29 記載の媒体。

31. ネットワークを介して情報の授受を行う情報処理を実行する
プログラムを格納又は伝送する媒体において、

15 第 1 のコンテンツと、第 1 のコンテンツに関連する所定デー
タとを送信する場合に、

 上記第 1 のコンテンツとは別の第 2 のコンテンツに適用され
る秘密鍵を用いて、上記所定データに電子署名を行い、

20 その電子署名された電子署名データを上記所定データに組み
合わせて送信する

ことを特徴とするプログラムを格納又は伝送する
媒体。

32. 上記プログラムは、さらに、

25 上記秘密鍵を用いた電子署名を、上記第 2 のコンテンツ又は
上記秘密鍵を管理する側に依頼し、その依頼に基づいて得られ
た電子署名データを、上記所定データに組み合わせること

を特徴とする請求項 31 記載の媒体。

33. 上記プログラムは、さらに、

上記秘密鍵を使用して電子署名が行われる上記所定データには、上記第 2 のコンテンツの参照命令を含ませること
を特徴とする請求項 3 1 記載の媒体。

34. 上記プログラムは、さらに、

5 上記所定データは、第 1 のコンテンツに対する挿入開始位置
情報、挿入終了位置情報及び対応する第 2 のコンテンツの参照
開始位置情報、参照終了位置情報を有すること
を特徴とする請求項 3 3 記載の媒体。

10 35. ネットワークを介して情報の授受を行い、それら情報を記録
及び／又は再生する情報処理を実行するプログラムを格納又は
伝送する媒体において、

 第 1 のコンテンツを記録するとき、上記第 1 のコンテンツに
関連する第 1 の所定データと、既に記録された第 2 のコンテン
ツに適用される秘密鍵を上記第 1 の所定データに用い生成され
15 た電子署名データとを記録する
 ことを特徴とするプログラムを格納又は伝送する
媒体。

36. 上記プログラムは、さらに、

20 上記秘密鍵を使用して電子署名が行われる上記第 1 の所定デ
ータには、第 2 のコンテンツの参照命令を含ませること
を特徴とする請求項 3 5 記載の媒体。

37. 上記プログラムは、さらに、

25 上記第 1 の所定データに、第 1 のコンテンツに対する挿入開
始位置情報、挿入終了位置情報及び対応する第 2 のコンテン
ツの参照開始位置情報、参照終了位置情報を含ませること
を特徴とする請求項 3 6 記載の媒体。

38. 上記プログラムは、さらに、

 第 2 のコンテンツと上記秘密鍵に対応する公開鍵とを受信し

たとき、受信された上記第 2 のコンテンツと上記公開鍵を記録
させること

を特徴とする請求項 3 5 記載の媒体。

39. 上記プログラムは、さらに、

5 上記電子署名データを上記公開鍵を用い復号化し、復号化デ
ータを生成し、

 上記第 1 の所定データを所定のアルゴリズムに基づいて第 2
の所定データに変換し、

 上記復号化データと上記第 2 の所定データとを照合すること
10

を特徴とする請求項 3 8 記載の媒体。

40. 上記プログラムは、さらに、

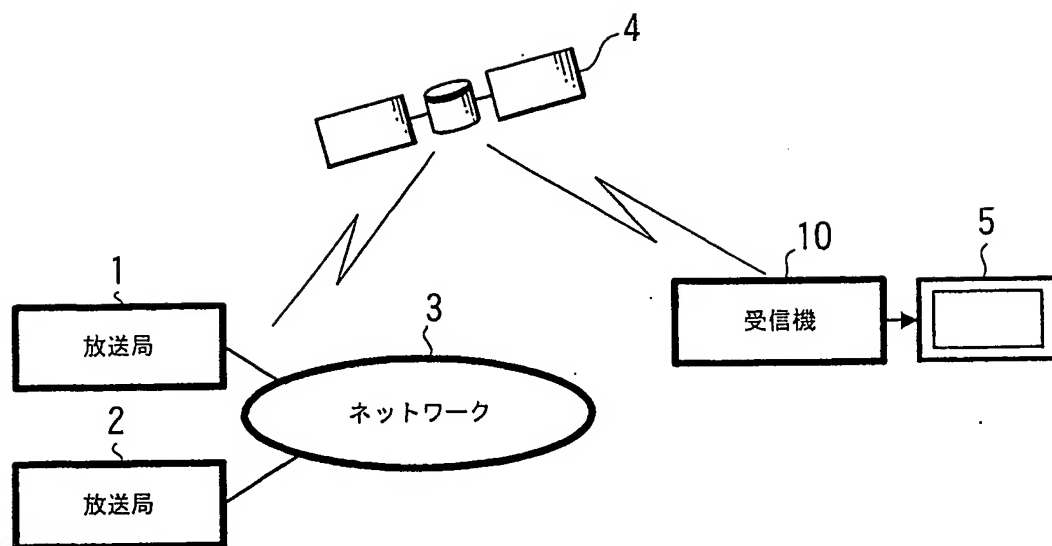
 上記照合の結果が一致した場合、上記第 1 の所定データに基
づき、既に記録された第 2 のコンテンツを所定のタイミングで
15 参照すること

を特徴とする請求項 3 9 記載の媒体。

20

25

FIG. 1



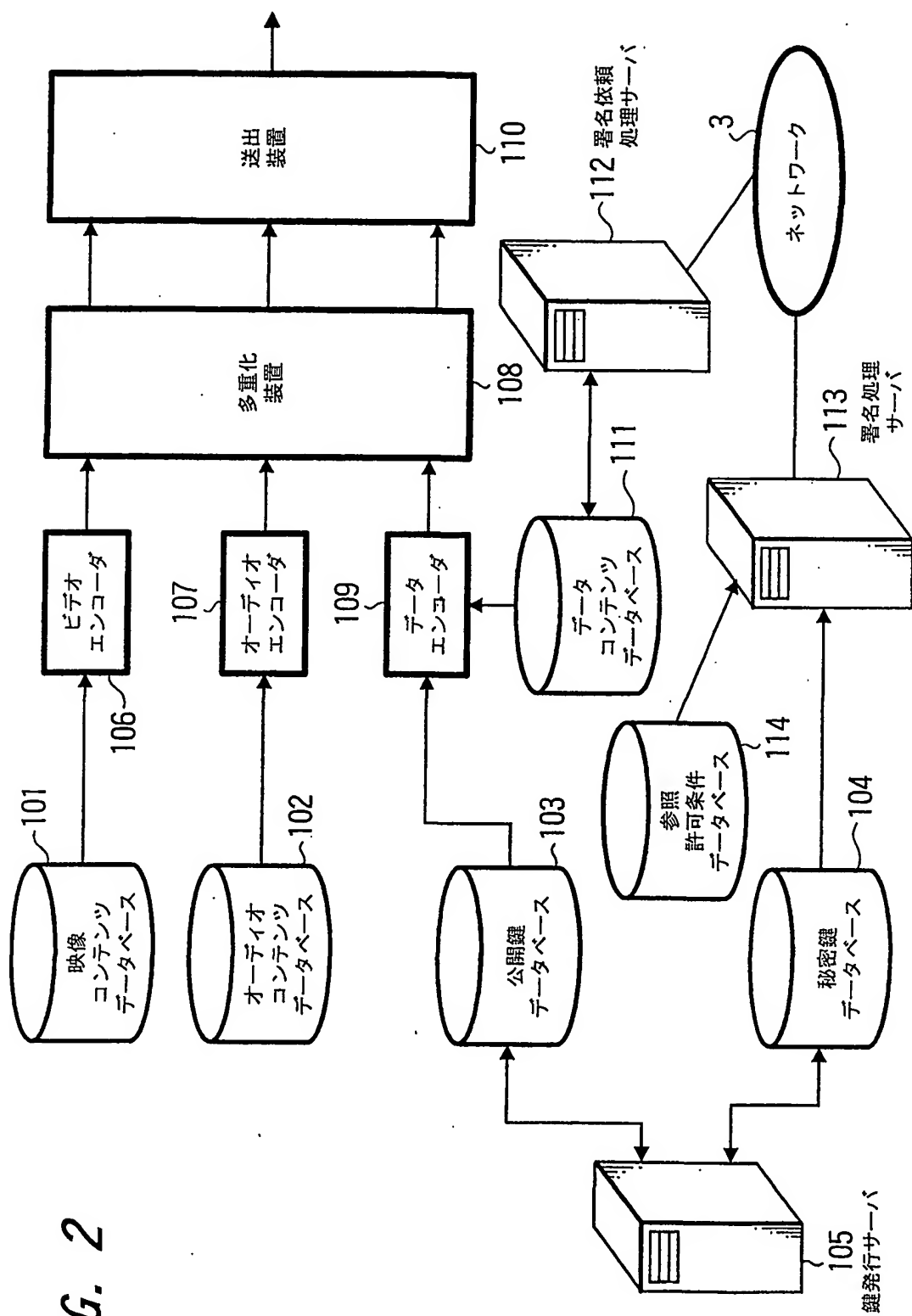
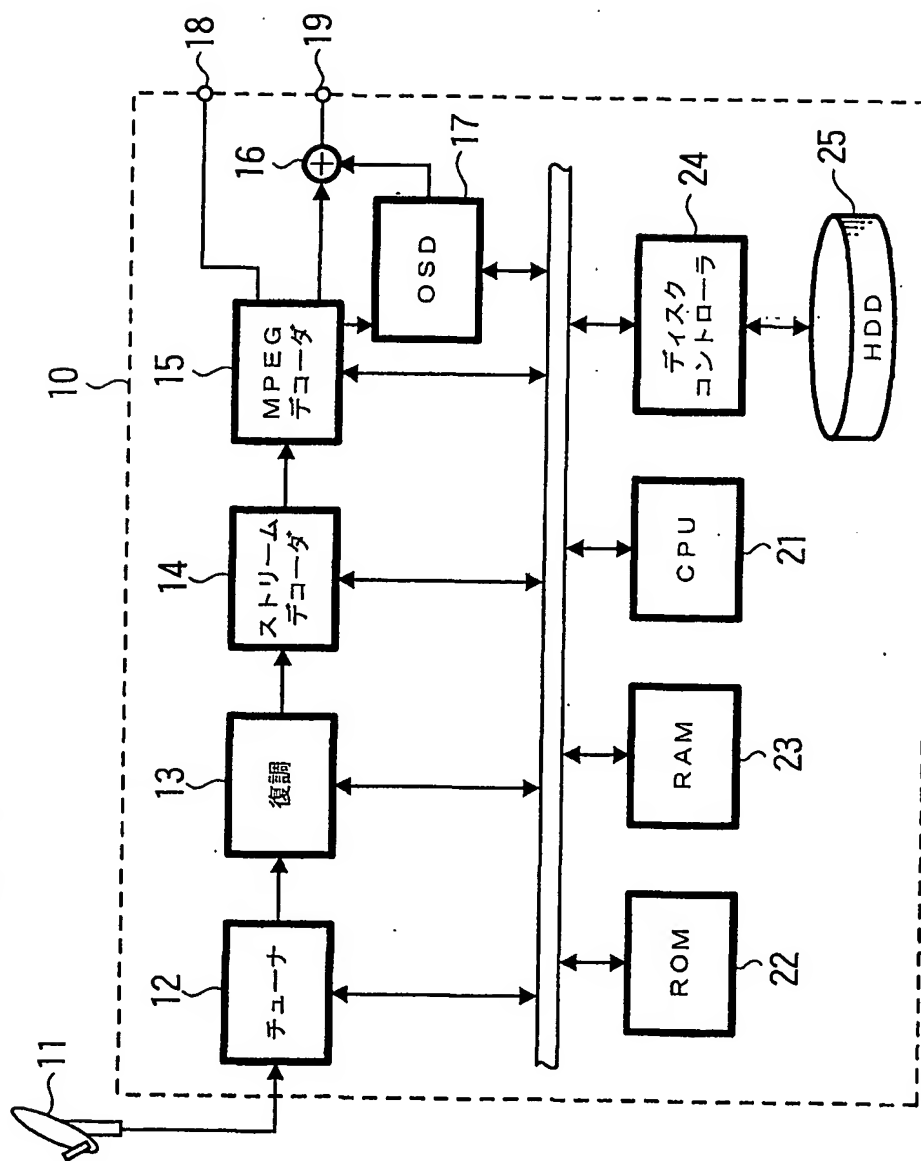


FIG. 3



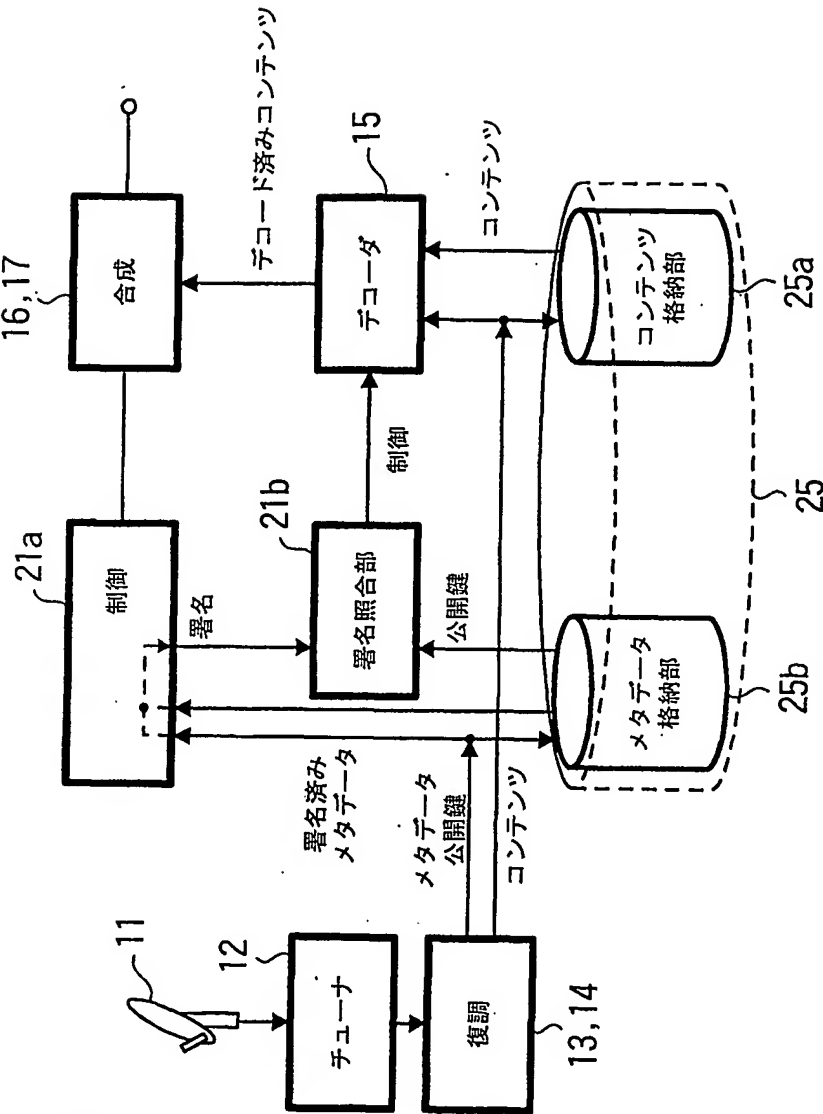


FIG. 4

FIG. 5

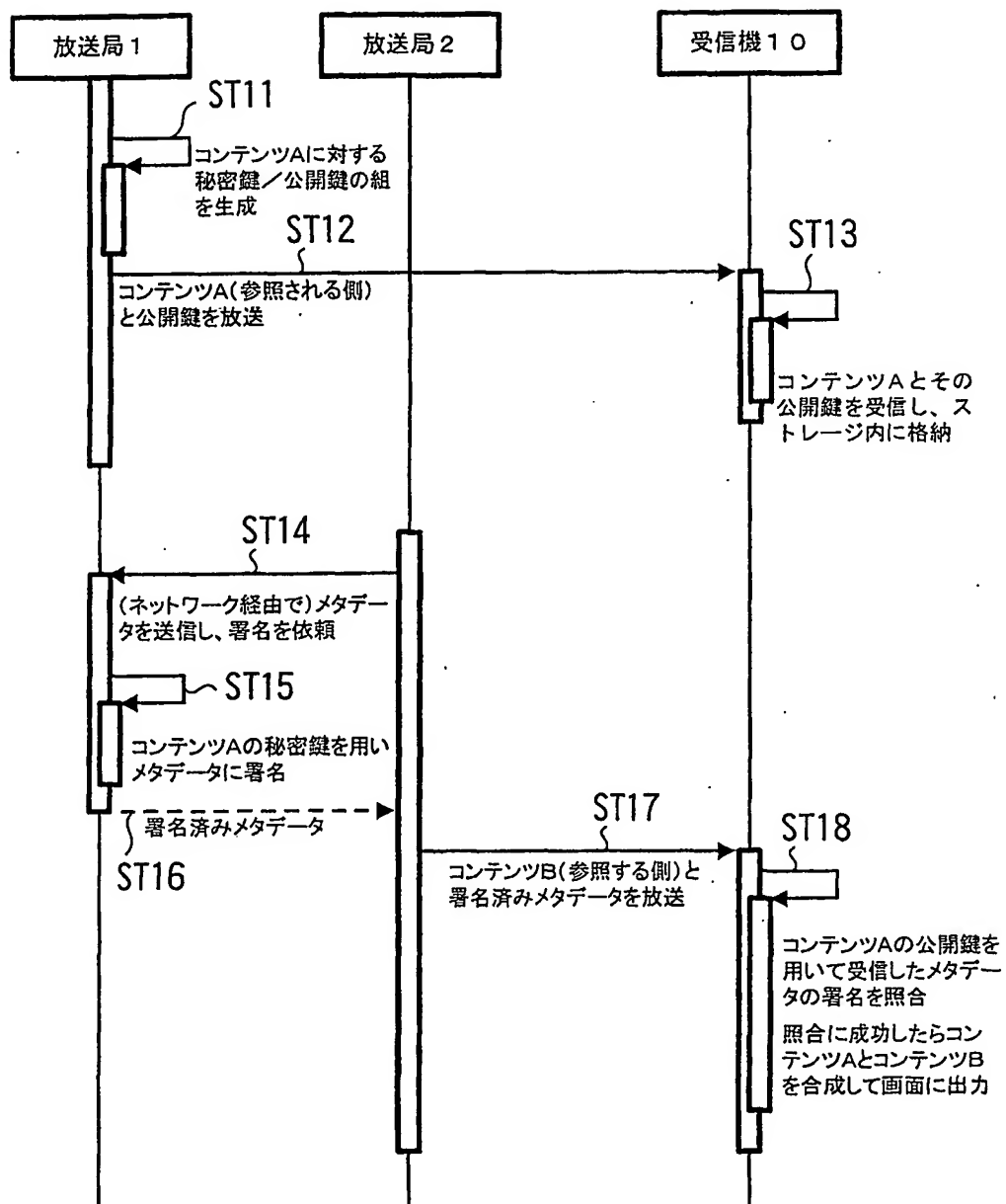


FIG. 6

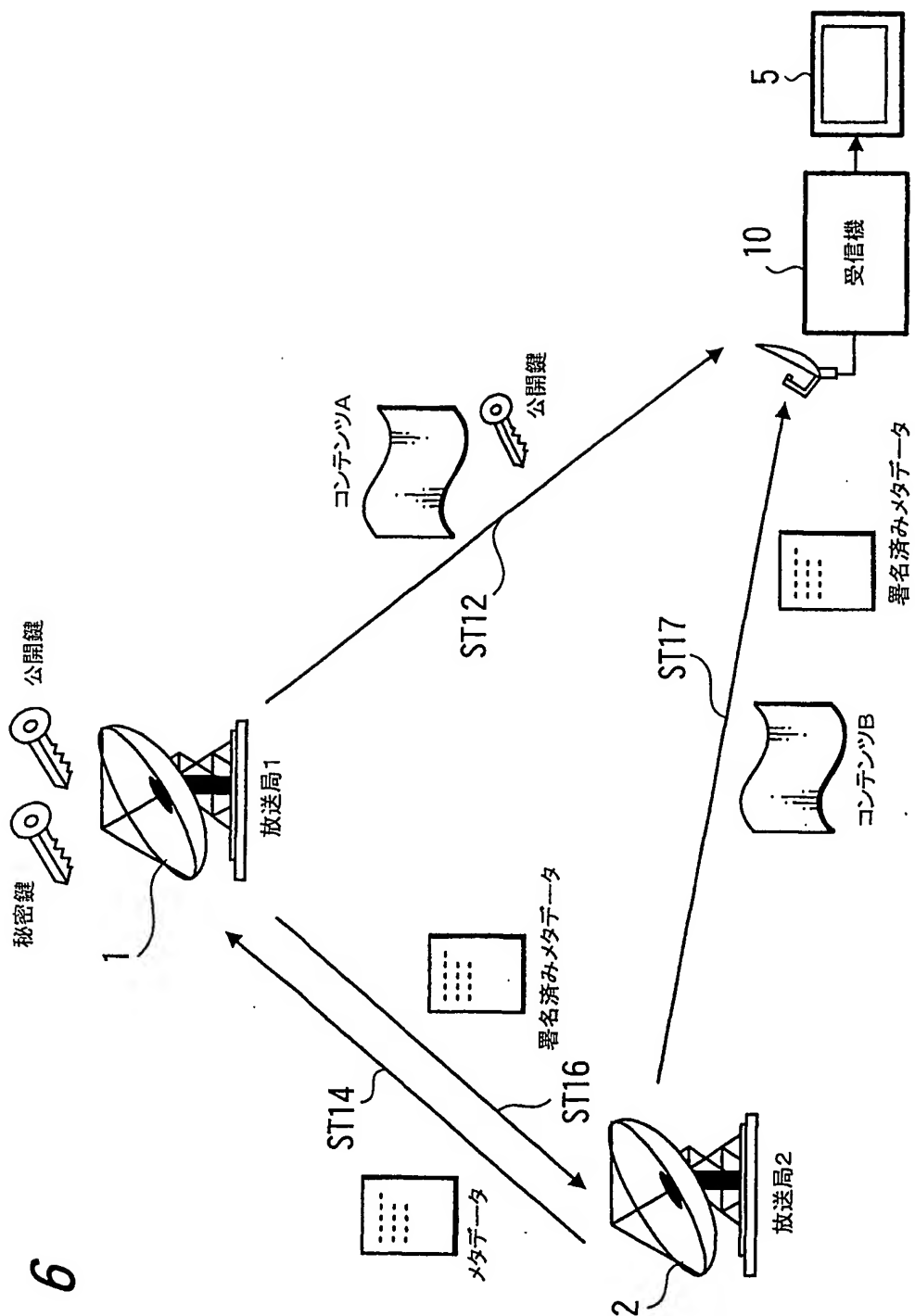


FIG. 7

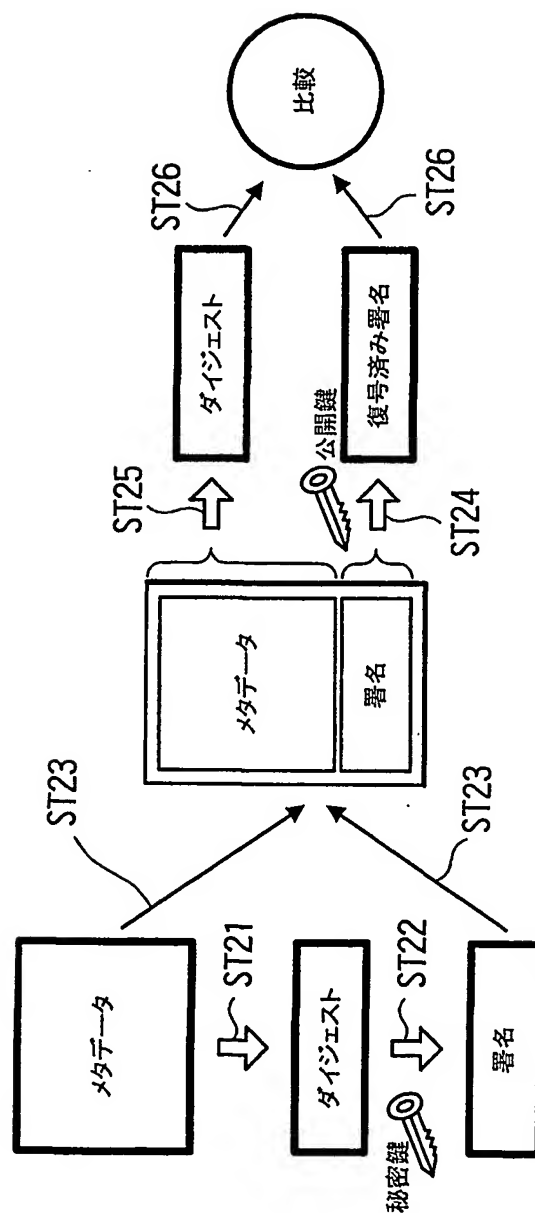


FIG. 8

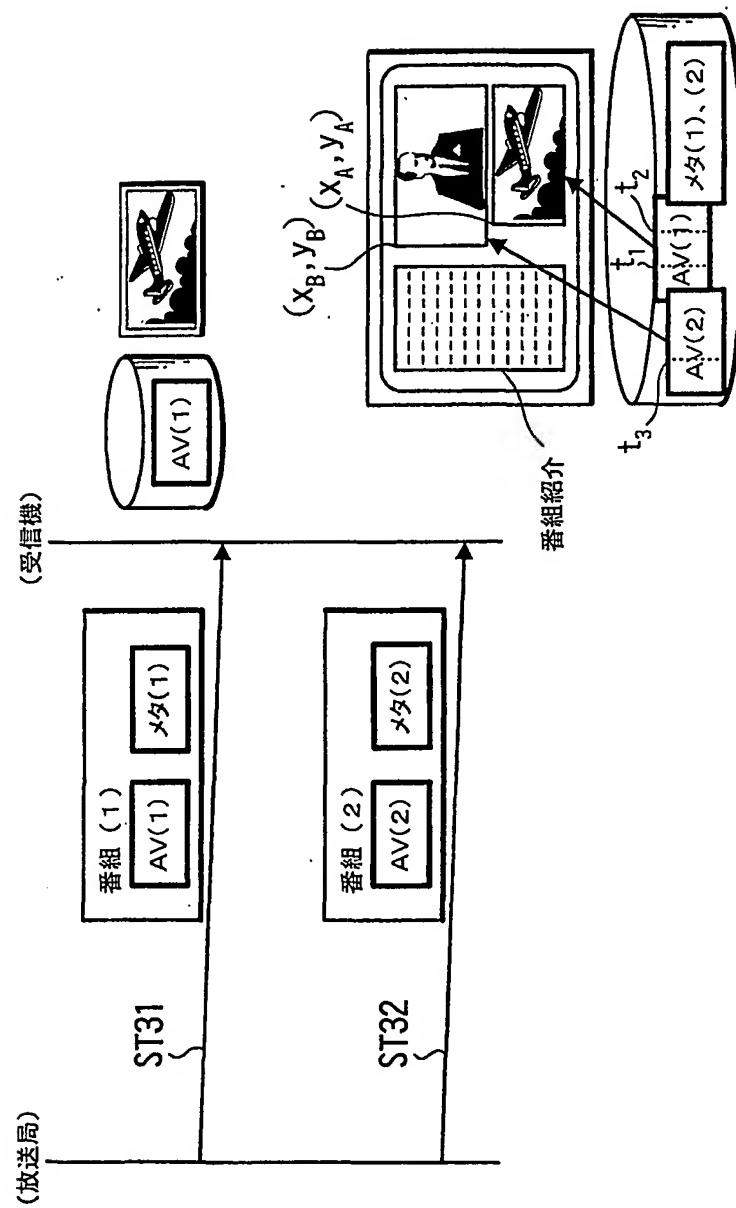


FIG. 9

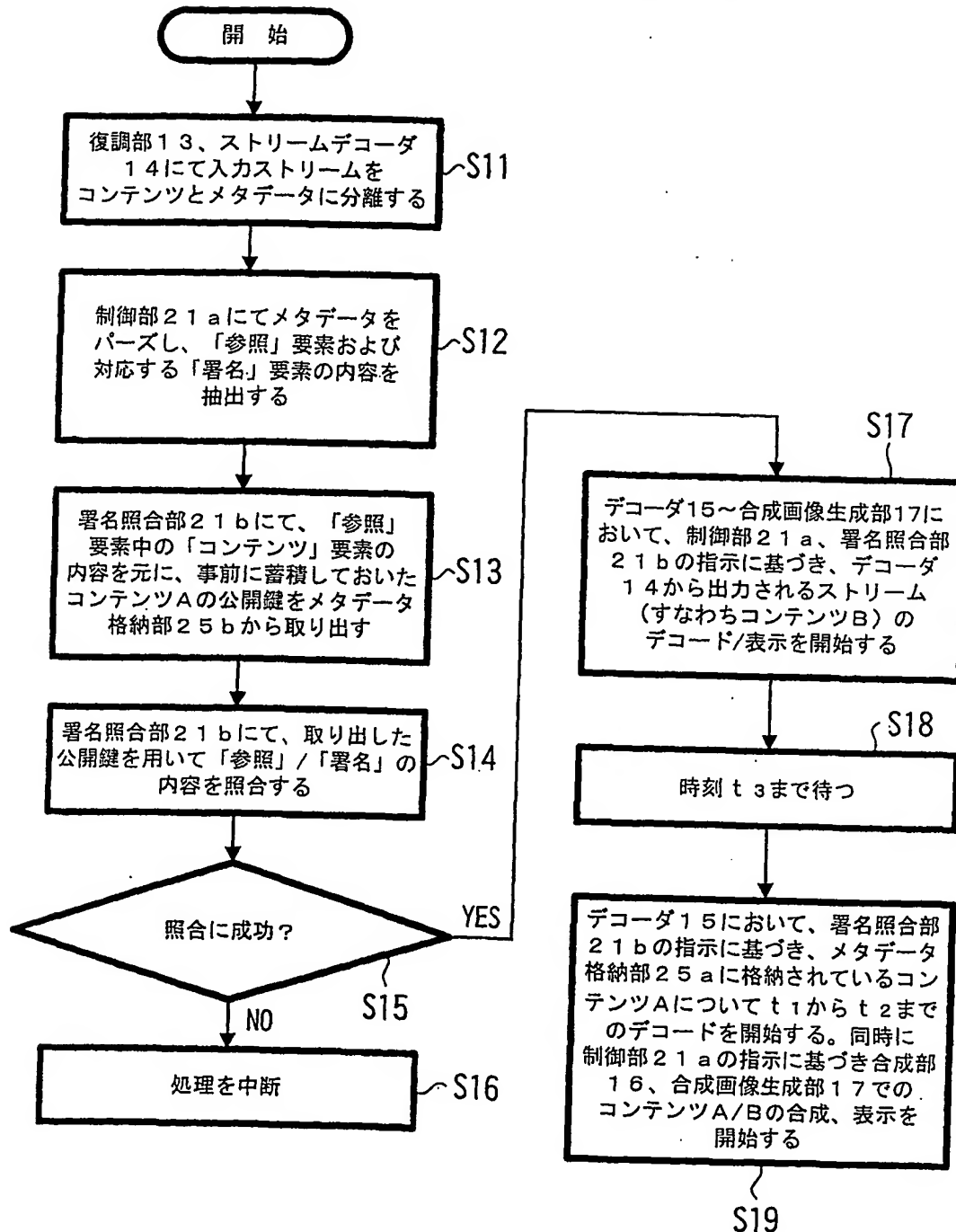
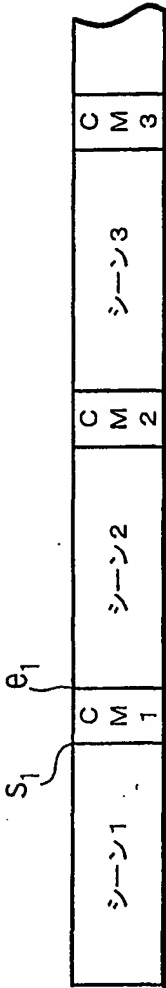
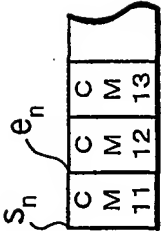


FIG. 10A



コンテンツA

FIG. 10B



コンテンツB

FIG. 10C



出力映像

FIG. 11

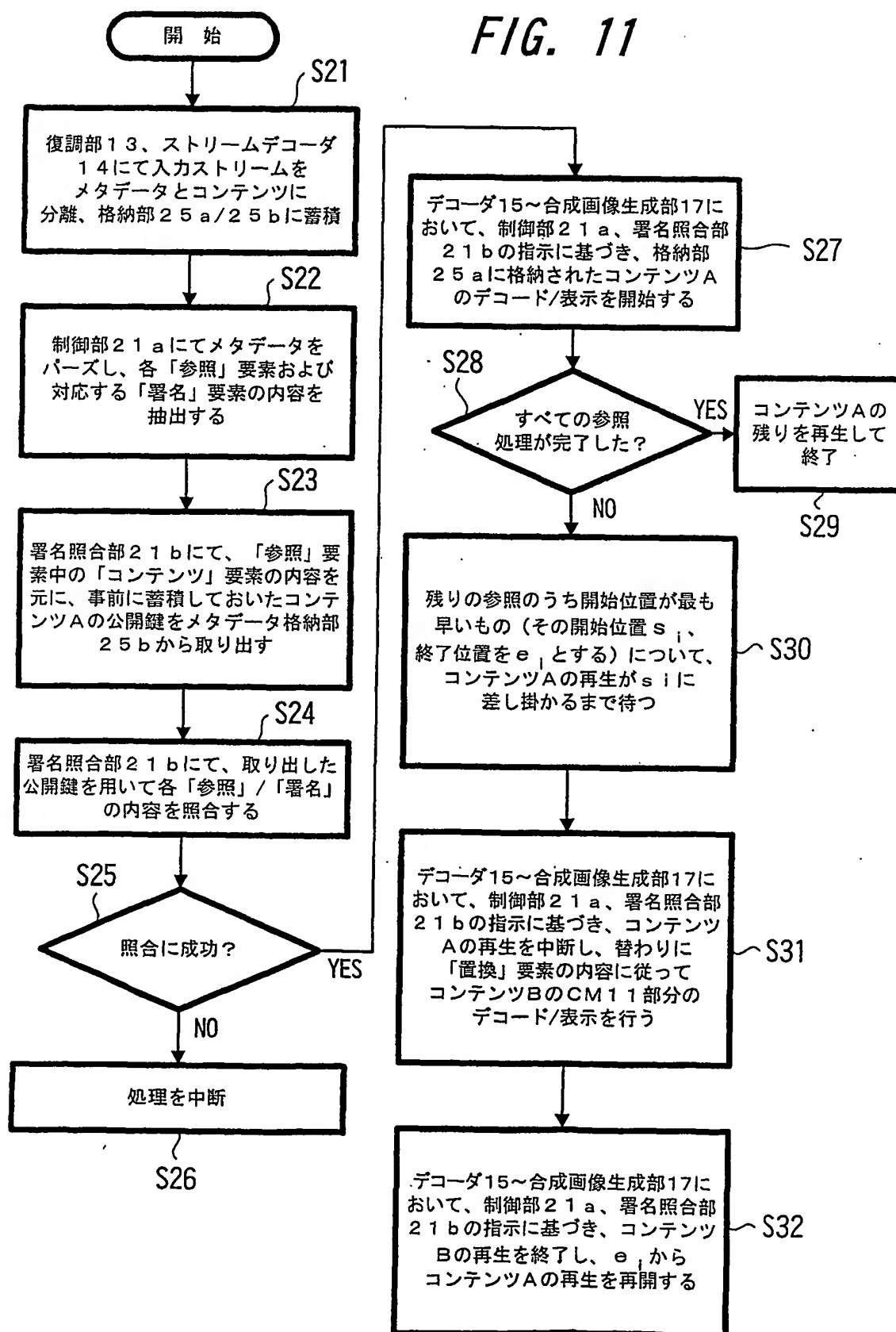
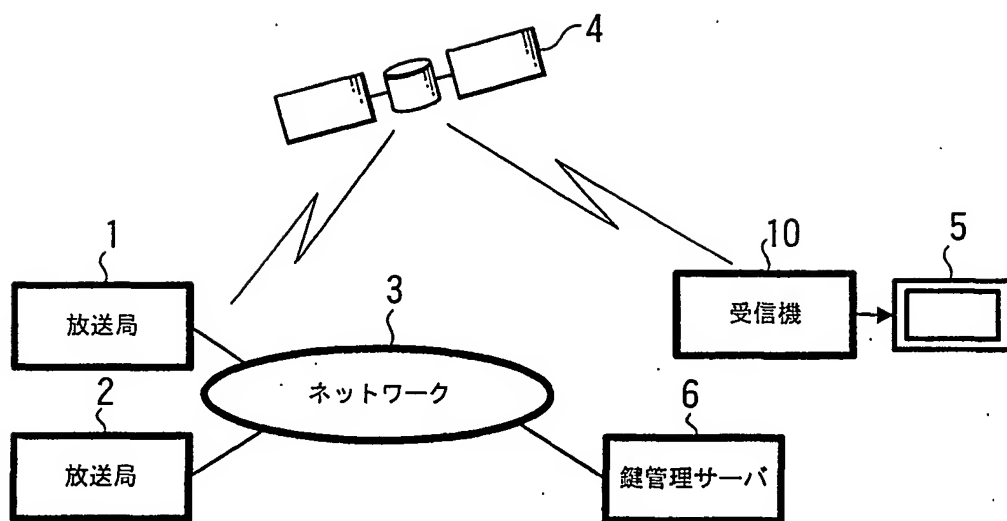
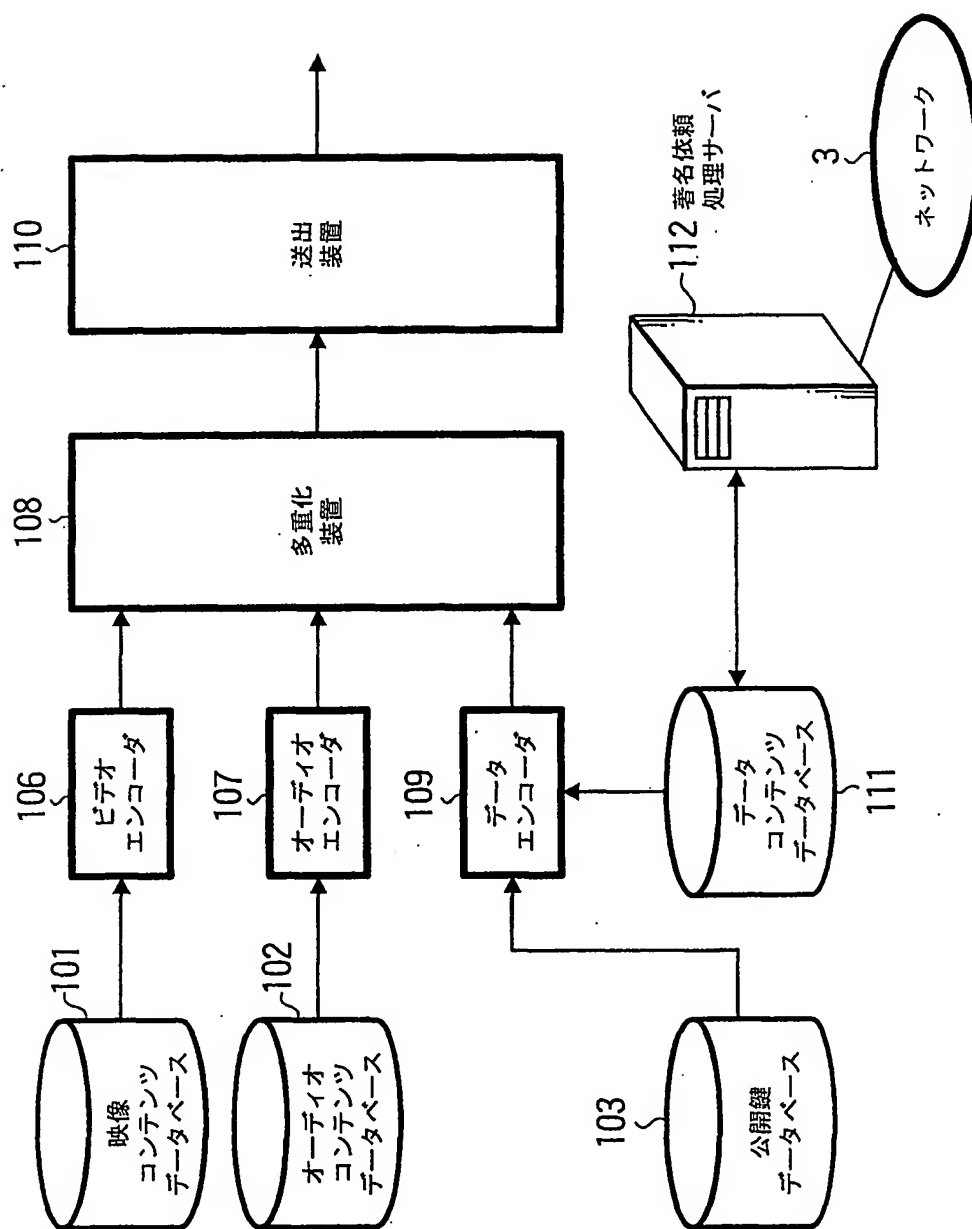


FIG. 12





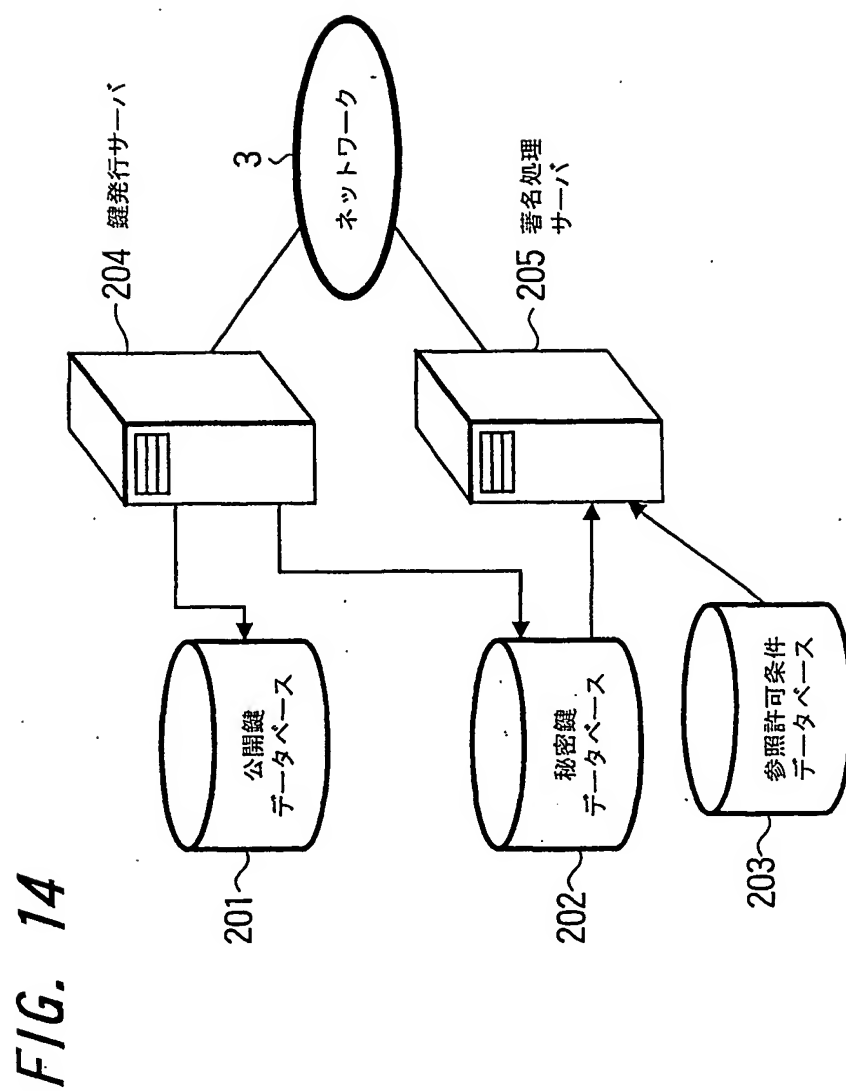


FIG. 15

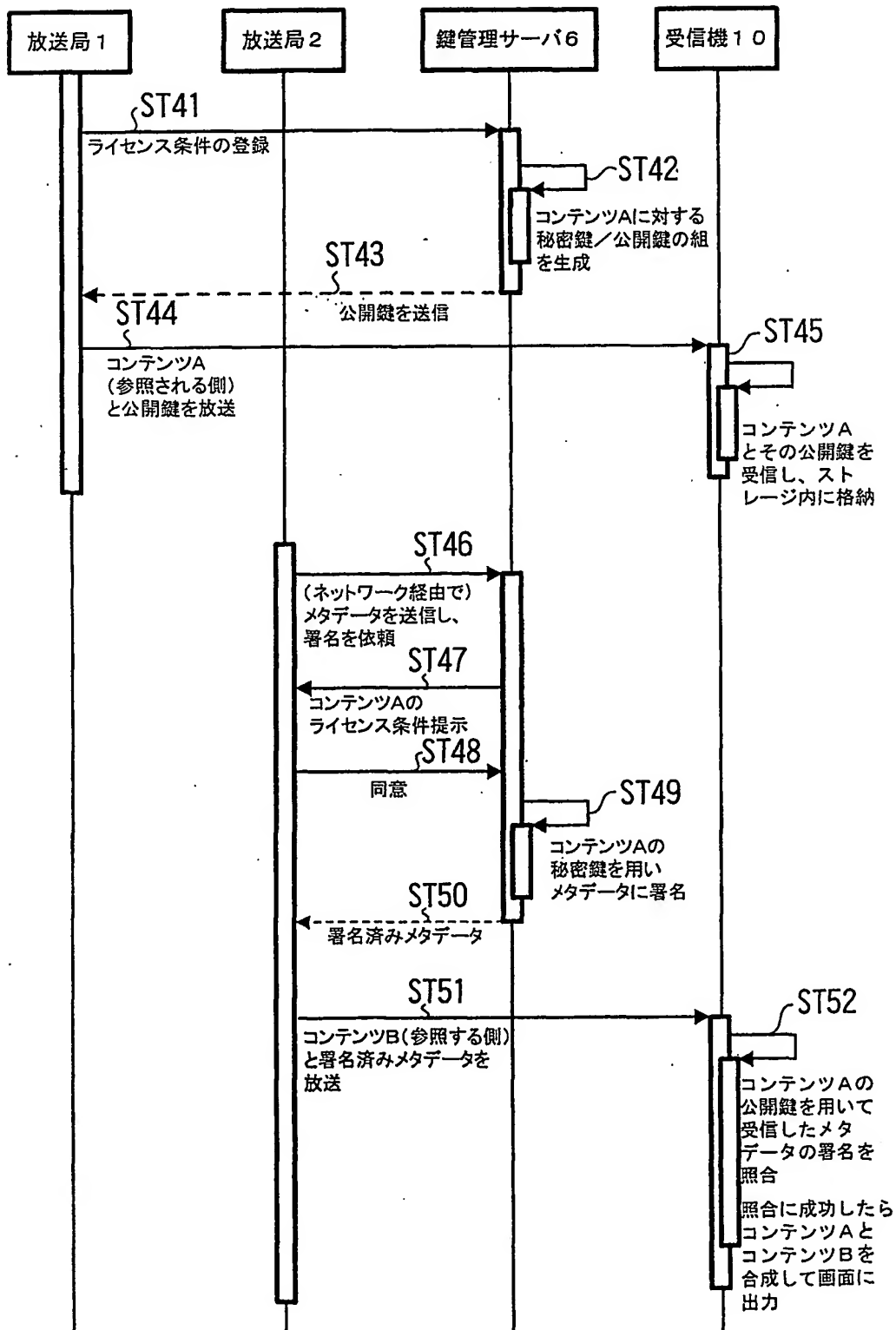
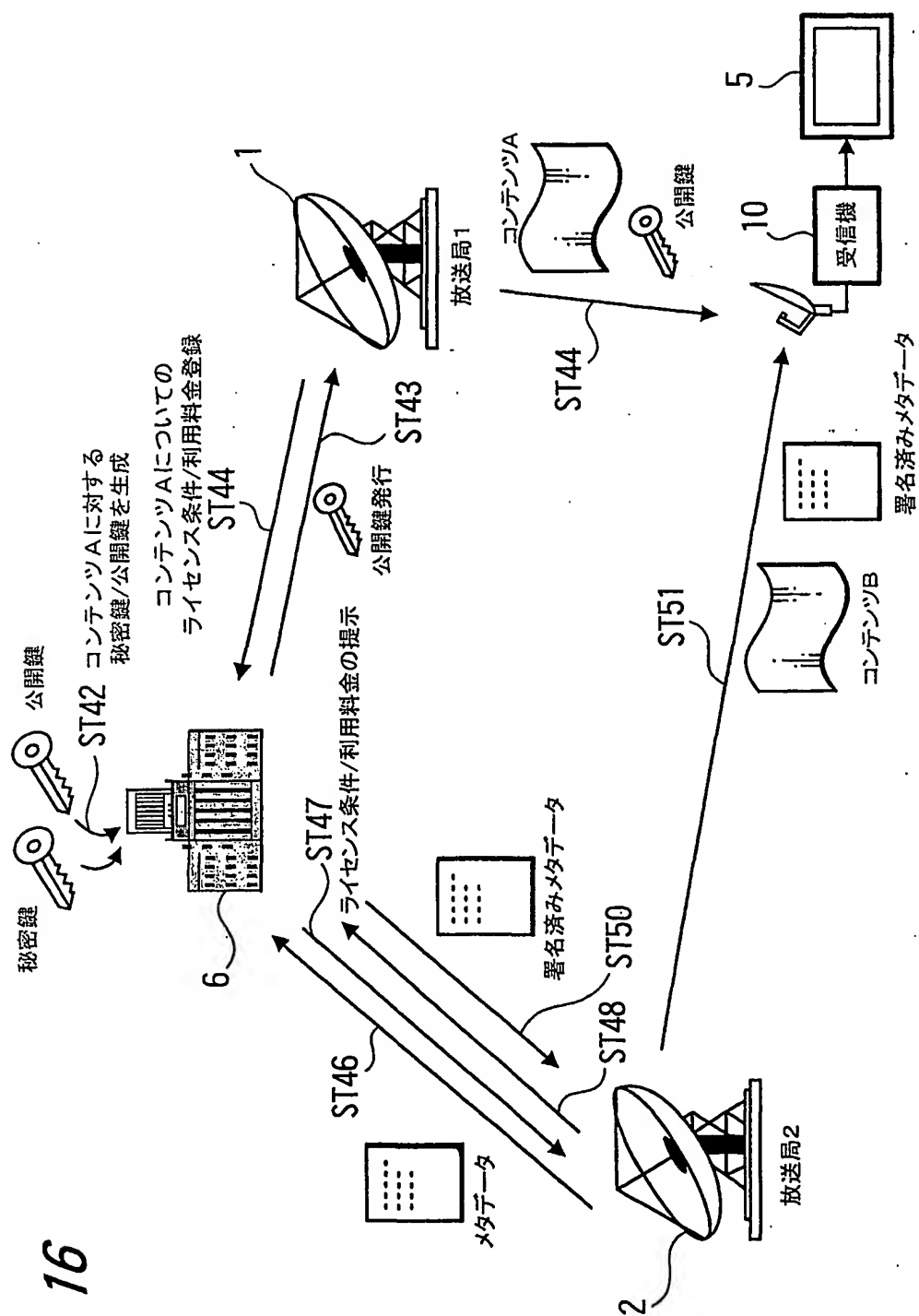


FIG. 16



引 用 符 号 の 説 明

1	第 1 の放送局
2	第 2 の放送局
3	ネットワーク
4	人工衛星
5	受像機
6	鍵管理サーバ
1 0	受信機
1 1	アンテナ
1 2	チューナ部
1 3	復調部
1 4	ストリームデコーダ
1 5	M P E G デコーダ
1 6	合成部
1 7	合成画像生成部
1 8	音声出力部
1 9	映像出力部
2 1	中央制御ユニット (C P U)
2 1 a	制御部
2 1 b	署名照合部
2 2	R O M
2 3	R A M
2 4	ディスクコントローラ
2 5	ハードディスクドライブ (H D D)
2 5 a	コンテンツ格納部
2 5 b	メタデータ格納部
1 0 1	映像コンテンツデータベース
1 0 2	オーディオコンテンツデータベース

1 0 3	公開鍵データベース
1 0 4	秘密鍵データベース
1 0 5	鍵発行サーバ
1 0 6	ビデオエンコーダ
1 0 7	オーディオエンコーダ
1 0 8	多重化装置
1 0 9	データエンコーダ
1 1 0	送出装置
1 1 1	データコンテンツデータベース
1 1 2	署名依頼処理サーバ
1 1 3	署名処理サーバ
2 0 1	公開鍵データベース
2 0 2	秘密鍵データベース
2 0 3	参照許可条件データベース
2 0 4	鍵発行サーバ
2 0 5	署名処理サーバ

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/07924

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04N7/10, 7/16-7/173, G06F15/00-15/00, 390Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-155735 A (Mitsubishi Electric Corporation), 06 June, 2000 (06.06.00), Full text; Figs. 7 to 8 (Family: none)	1-40
Y A	JP 10-13811 A (Matsushita Electric Ind. Co., Ltd.), 16 January, 1998 (16.01.98), Full text; Figs. 1 to 70 & EP 817105 A2 & US 6035304 A	1-6, 11-40 7-10
Y A	JP 11-96064 A (Nippon Telegr. & Teleph. Corp. <NTT>), 09 April, 1999 (09.04.99), Full text; Figs. 1 to 9 (Family: none)	5, 6, 12, 13, 21, 22, 24, 25, 33, 34, 36, 37 1-4, 7-11, 14-20, 23, 26-32, 35, 38-40
Y A	JP 10-290443 A (Nippon Telegr. & Teleph. Corp. <NTT>), 27 October, 1998 (27.10.98), Full text; Figs. 1 to 11 (Family: none)	7-10 1-6, 11-40

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 10 December, 2001 (10.12.01)	Date of mailing of the international search report 18 December, 2001 (18.12.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/07924

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 8-340525 A (Toshiba Corporation), 24 December, 1996 (24.12.96), Full text; Figs. 1 to 5 (Family: none)	7-10 1-6, 11-40
A	JP 11-212462 A (Canon Inc.), 06 August, 1999 (06.08.99), Full text; Figs. 1 to 16 & EP 932298 A2 & CN 1239378 A	1-40

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl ⁷ H04N7/16		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl ⁷ H04N7/10, 7/16-7/173, G06F15/00-15/00, 390		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2001年 日本国登録実用新案公報 1994-2001年 日本国実用新案登録公報 1996-2001年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J.P. 2000-155735 A (三菱電機株式会社) 6. 6 月. 2000 (06. 06. 00) 全頁, 第7-8図 (ファミリーなし)	1-40
Y A	J.P. 10-13811 A (松下電器産業株式会社) 16. 1 月. 1998 (16. 01. 98) 全頁, 第1-70図 &EP 817105 A2 &US 6035304 A	1-6, 11-40 7-10
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	国際調査報告の発送日	
10. 12. 01	18.12.01	
国際調査機関の名称及びあて先	特許庁審査官 (権限のある職員)	5 P 9746
日本国特許庁 (ISA/JP)	古川 哲也	
郵便番号100-8915		
東京都千代田区霞が関三丁目4番3号	電話番号 03-3581-1101	内線 3581

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 . 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	J P 11-96064 A (日本電信電話株式会社) 9. 4月. 1999 (09. 04. 99) 全頁, 第1-9図 (ファミリーなし)	5, 6, 12, 13, 21, 22, 24, 25, 33, 34, 36, 37 1-4, 7-11, 14- 20, 23, 26-32, 35, 38-40
Y A	J P. 10-290443 A (日本電信電話株式会社) 27. 1 0月. 1998 (27. 10. 98) 全頁, 第1-11図 (ファミリーなし)	7-10 1-6, 11-40
Y A	J P. 8-340525 A (株式会社東芝) 24. 12月. 19 96 (24. 12. 96) 全頁, 第1-5図 (ファミリーなし)	7-10 1-6, 11-40
A	J P 11-212462 A (キヤノン株式会社) 6. 8月. 1 999 (06. 08. 99) 全頁, 第1-16図 & E P. 932298 A2 & C N 1239378. A	1-40